



Council of the  
European Union

Brussels, 22 May 2018  
(OR. en)

---

---

**Interinstitutional File:**  
**2017/0002 (COD)**

---

---

8394/1/18  
REV 1

**LIMITE**

**DATAPROTECT 73**  
**JAI 342**  
**DAPIX 119**  
**EUROJUST 45**  
**FREMP 56**  
**ENFOPOL 189**  
**COPEN 118**  
**DIGIT 76**  
**RELEX 345**  
**CODEC 642**  
**FRONT 143**

#### **NOTE**

From:	Presidency
To:	Permanent Representative Committee
No. prev. doc.:	5034/17; WK 5375/2018
Subject:	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC [First reading] <b>- Preparation for the trilogue</b>

#### **I. INTRODUCTION**

On 10 January 2017, the Commission adopted the above-mentioned proposal for a Regulation which lays down rules on the processing of personal data by Union institutions, bodies, offices and agencies as well as on the free movement of personal data in the Union. The proposal also lays down the provisions on the European Data Protection Supervisor (EDPS). The EDPS monitors the application of the Regulation to all processing of personal data carried out by Union institutions, bodies, offices and agencies.

This Regulation on data protection by Union institutions and bodies adds to the modernized EU data protection regime. In April 2016, the Council and the European Parliament adopted the so-called 'data protection package' which comprises the General Data Protection Regulation 2016/679 (GDPR) and the Law Enforcement Directive 2016/680 on data protection for law enforcement purposes. The Regulation on data protection by Union institutions and bodies should be aligned with the GDPR and the Law Enforcement Directive as far as possible. The GDPR applies as of 25 May 2018. Member States had until 6 May to adopt and publish the national laws transposing the Law Enforcement Directive.

In June 2017, under Maltese Presidency, the Justice and Home Affairs Council adopted the General Approach on the proposed Regulation (9091/17) thereby giving the Presidency a negotiating mandate to enter into trilogues. The European Parliament adopted its negotiating position in October 2017. trilogues started under Estonian Presidency and continued under Bulgarian Presidency.

At the trilogue on 16 May 2018, the Presidency and the Rapporteur succeeded in solving most of the outstanding issues. The few minor issues that remain open are to be solved at the technical meeting on 22 May. In addition to the compromise text contained in the fourth column of the table that appears in Annex, the Presidency will submit the outcome of the technical meeting for endorsement to the meeting of the Committee so that, on 23 May, it can examine the compromise package in its entirety. On those remaining minor issues, the Presidency will insist that the European Parliament accepts the Council compromise suggestions as presented in the fourth column.

Because of the strong link between the draft Regulation and the GDPR, it is important that the EU co-legislators find agreement on the draft Regulation before 25 May 2018.

## **II. COMPROMISE PACKAGE**

The Presidency considers that the compromise package respects all Council's priorities. The package sets out a general data protection regime for Union institutions and bodies that is aligned with the GDPR. As regards the Union agencies, offices and bodies carrying out activities in the field of judicial cooperation in criminal matters and police cooperation, it creates specific data protection rules that are consistent with the Law Enforcement Directive, taking account of the specific needs in line with Declaration No 21 attached to the Lisbon Treaty.

### **1. Main political issues**

The compromise package consists of four main political issues:

- A. Scope of the Regulation and Chapter VIIIA on processing of operational personal data;
- B. Internal rules enabling Union institutions and bodies to restrict rights of data subjects;
- C. Short-list of EDPS candidates;
- D. Coordinated supervision model.

#### **A. Scope and Chapter VIIIA on processing of operational personal data**

The most important political issue concerns processing of operational personal data by agencies carrying out activities in the field of judicial cooperation in criminal matters and police cooperation. On the one hand, to reduce fragmentation of data protection rules, the European Parliament considered that all processing of personal data by Union agencies in this specific field (Eurojust, Europol and the European Public Prosecutor's Office (EPPO) and possibly other agencies carrying out law enforcement activities) must be laid down in the new Regulation. On the other hand, because of the specific needs of law enforcement agencies when processing personal data, the Council wanted these agencies to continue to have specific data protection rules for their operations in their founding acts. In order to converge the positions of the Council and the Parliament, the trilogue agreed on inserting in the Regulation a new Chapter VIIIA with general rules on processing of operational personal data by Union agencies, offices and bodies when carrying out activities in the field of judicial cooperation in criminal matters and police cooperation, while retaining specific tailor-made provisions in the founding acts of the agencies.

The Presidency considers that the compromise can be endorsed as it meets all Council's key priorities:

- The application of the principle of *lex specialis derogat legi generali* provides the necessary legal certainty as the provisions laid down in Chapter VIIIa on processing of operational personal data in the Regulation are without prejudice to the provisions of the founding acts of the agencies in the field of judicial cooperation in criminal matters and police cooperation and other Union legal acts applicable to them;
- Europol and the EPPO as well as the Common Security and Defence Policy missions are excluded from the scope of the Regulation.
- The substantial provisions in Chapter VIIIa on processing of operational personal data are identical or are very close to the rules of the Law Enforcement Directive 2016/680;
- Chapter VIIIa is a separate chapter and the other provisions of the Regulation, except the definitions in Article 3, do not apply to processing of operational personal data when carrying out activities in the field of judicial cooperation in criminal matters and police cooperation.

The regime this compromise sets out will be assessed in due time as Article 70 b provides that, by May 2022, the Commission will review the Regulation and other legislative acts relating to processing of operational personal data. On the basis of that review, the Commission may submit appropriate legislative proposals.

At the trilogue on 16 May, the Presidency and the Rapporteur agreed to amend certain provisions in Chapter VIIIa:

**Article 69h (processing of special categories of operational personal data).**

In order to avoid that law enforcement agencies can only process personal data that are linked to personal data already in their possession, at the end of Article 69h, the phrase suggested by the EP ("and only if those data supplement other personal data already processed by the controller") is deleted. Furthermore, to accommodate the EP, as a last sentence, a provision is inserted prohibiting discrimination of natural persons on the basis of such personal data.

### **Article 68i (automated individual decision-making).**

The text of the Article is fully aligned with Article 11 of the Law Enforcement Directive 2016/680.

### **Article 69ma (right of access in criminal investigations and proceedings).**

The compromise text introduces stronger wording to ensure the necessary close cooperation between the national competent authority and the Union Agency in relation to a data subject right of access request. As a result, the Union agencies remain responsible for the decision about access to the personal data while, at the same time, the national competent authority concerned is closely involved in that decision.

### **Article 69q (supervision by the European Data Protection Supervisor).**

The exercise of the supervisory powers of the European Data Protection Supervisor is limited as he or she must take "utmost account of the secrecy of judicial inquiries and criminal proceedings in accordance with Union or Member State law".

In addition to changes in Chapter VIIIA, the trilogue made minor changes to **Recital (53) and Articles 48(1), 49(1) and 51(1)**. In order to allow agencies which do not operate under Chapter VIIIA to transfer personal data to law enforcement entities in third countries a reference to the adequacy decision under the Law Enforcement Directive is added in these four provisions.

### **B. Internal rules (Article 25)**

Restrictions to data subject rights are laid down in Article 25 of the compromise package. EU institutions and bodies may restrict data subject rights via legal acts adopted on the basis of the Treaties or via internal rules. For these internal rules to be compliant with Article 52(1) of the Charter of Fundamental Rights, which provides that limitations of rights must be set out in law, the Council qualified these rules by providing that they shall be clear and precise acts of general application, intended to produce legal effects vis-a-vis data subjects, adopted at the highest level of management of the Union institutions and bodies and subject to publication in the Official Journal of the European Union. In addition, it is specified in Article 41(2) of the general approach that Union institutions and bodies must consult the EDPS when drawing up their internal rules. Finally, it is noted that the Council, like the European Parliament, deleted the provision on *ad hoc* restrictions laid down in Article 25(2) of the Commission proposal.

Initially, the European Parliament could not accept that Union institutions and bodies use internal rules to restrict fundamental rights like the right to protection of personal data. The Parliament is now willing to accept the Council's general approach as regards internal rules. However, the Parliament links agreement on internal rules to agreement on transparency (see below).

C. Shortlist EDPS candidates (Article 54(1) and Article 54(2)).

The trilogue suggests that the list of EDPS candidates drawn up by the Commission shall be public and shall consist of at least three candidates. Moreover, the EDPS should have specific data protection expertise.

D. Coordinated supervision model (Article 62)

On the one hand, the Commission proposed a single model for coordinated supervision of Union institutions and bodies and large IT systems by the EDPS and the national data protection authorities. Central in this coordination is the European Data Protection Board. The coordinated supervision model would apply where a Union founding act of a Union institution or body or large IT system refers to Article 62 of the Regulation. In its general approach, the Council followed the same incremental approach as the Commission. On the other hand, the EP suggested to apply the harmonised cooperation model, already now, to all Union institutions and bodies and large IT systems mentioned in its amendments to the Regulation. In a spirit of compromise, the Parliament, whilst improving the wording of the Commission proposal tentatively accepted the arrangement set out in the Council general approach.

## **2. Minor political issues**

The following minor political issues remain outstanding because the trilogue on 16 May had insufficient time to discuss them:

- Transparency and transmission to recipients other than Union institutions and bodies (Recital 22, Articles 9(1) and 70a);
- EDPS consultation in preparation of a Commission proposal (Recital (50) and Article 42(1));
- Transfers between Union institutions and bodies (Article 8a);
- Data Protection Officer (Article 44(4)).

Already in December 2017, the Council took a position on the above-mentioned issues (15961/17). The Presidency will reiterate that position at the technical meeting on 22 May with a view to having the EP accept the Council compromise suggestions.

The trilogue on 16 May did discuss the minor political issue of the **Central Register** (Recitals (42) and (47) and Article 31(5)) and agreed that Union institutions and bodies shall keep their records of processing activities in a central register, unless it is not appropriate taking into account the size of the institution or agency. Moreover, the Union institutions and bodies are obliged to make the register publicly accessible.

Although the trilogue did not discuss the minor political issue of **Transparency and transmission to recipients other than Union institutions and bodies**, the Presidency submits new compromise text with a view to finding a compromise with the European Parliament at the technical meeting on 22 May. Building on the Council text on the Articles 9(1) and 70a and recital (22) of December 2017, the Presidency suggests a new compromise text that fully takes into account the case-law on access to public documents containing personal data, in particular as regards the question of distribution of the burden of proof between, on the one hand, the recipient other than a Union institution or body and, on the other hand, the controller processing the data. The Presidency also suggests to move the text of the Council general approach in Article 70a to paragraph 3 of Article 9, given that it deals with the same issue as Article 9(1), in particular littera (b).

Finally, the Presidency suggests to align the **date of application** of the Regulation with the date of entry into force. For that reason, paragraph 2 of Article 73 is deleted. By default, the Regulation starts to apply from the date of entry into force.

### **III. CONCLUSION**

The Presidency considers that the compromise text as it appears in Annex meets all Council's priorities. Furthermore, both co-legislators share a strong political interest to announce a political agreement on the new rules for personal data protection in the EU institutions and bodies before the political deadline of 25 May 2018, the date of application of the GDPR.

Against that background, the Presidency invites the Committee of Permanent Representatives to endorse the compromise package resulting from the trilogue of 16 May. This document, and in particular its Annex, will be revised to take account of the outcome of the 22 May technical meeting. The Presidency will use the result of the analysis by the Committee with a view to reaching agreement with the European Parliament in the trilogue that will take place in the afternoon of 23 May.

In case agreement on an overall compromise text is found in the trilogue, the Presidency will submit this text to a forthcoming meeting of the Committee with the request to mandate the Committee's Chair to inform the Chair of the EP Committee on Civil Liberties, Justice and Home Affairs that, should the EP adopt its position at first reading in the form set out in the agreed text (subject to revision by the legal linguists of both institutions), the Council would approve this text.



Proposal for a

**REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**

**on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC**

<b>COM (2017) 8</b>	<b>EP Position / First Reading</b>	<b>Council General Approach</b>	<b>Final compromise</b>
THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,	THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,	THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,	
Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16(2) thereof,	Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16(2) thereof,	Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16(2) thereof,	
Having regard to the proposal from the European Commission,	Having regard to the proposal from the European Commission,	Having regard to the proposal from the European Commission,	
After transmission of the draft legislative act to the national parliaments,	After transmission of the draft legislative act to the national parliaments,	After transmission of the draft legislative act to the national parliaments,	
Having regard to the opinion of the European Economic and Social Committee <sup>1</sup> ,	Having regard to the opinion of the European Economic and Social Committee <sup>1</sup> ,	Having regard to the opinion of the European Economic and Social Committee <sup>1</sup> ,	

<sup>1</sup> OJ C , , p. .

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
Acting in accordance with the ordinary legislative procedure,	Acting in accordance with the ordinary legislative procedure,	Acting in accordance with the ordinary legislative procedure,	
Whereas:	Whereas:	Whereas:	
<p>(1)</p> <p>The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the ‘Charter’) and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning them.</p>	<p><b>AM 1</b></p> <p>(1)</p> <p>The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the ‘Charter’) and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning them. <i><b>This right is also guaranteed under Article 8 of the European Convention on Human Rights</b></i></p>	<p>(1)</p> <p>The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the ‘Charter’) and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning them.</p>	<p>(1)</p> <p>everyone has the right to the protection of personal data concerning them. This right is also guaranteed under Article 8 of the European Convention on Human Rights.</p> <p style="text-align: right;">T</p>
<p>(2)</p> <p>Regulation (EC) No 45/2001 of the</p>	<p>(2)</p> <p>Regulation (EC) No 45/2001 of the</p>	<p>(2)</p> <p>Regulation (EC) No 45/2001 of the</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
European Parliament and of the Council <sup>2</sup> provides natural persons with legally enforceable rights, specifies the data processing obligations of controllers within the Community institutions and bodies, and creates an independent supervisory authority, the European Data Protection Supervisor, responsible for monitoring the processing of personal data by the Union institutions and bodies. However, it does not apply to the processing of personal data in the course of an activity of Union institutions and bodies which fall outside the scope of Union law.	European Parliament and of the Council <sup>2</sup> provides natural persons with legally enforceable rights, specifies the data processing obligations of controllers within the Community institutions and bodies, and creates an independent supervisory authority, the European Data Protection Supervisor, responsible for monitoring the processing of personal data by the Union institutions and bodies. However, it does not apply to the processing of personal data in the course of an activity of Union institutions and bodies which fall outside the scope of Union law.	European Parliament and of the Council <sup>2</sup> provides natural persons with legally enforceable rights, specifies the data processing obligations of controllers within the Community institutions and bodies, and creates an independent supervisory authority, the European Data Protection Supervisor, responsible for monitoring the processing of personal data by the Union institutions and bodies. However, it does not apply to the processing of personal data in the course of an activity of Union institutions and bodies which fall outside the scope of Union law.	
(3)  Regulation (EU) 2016/679 of the European Parliament and of the Council <sup>3</sup> and Directive (EU)	(3)  Regulation (EU) 2016/679 of the European Parliament and of the Council <sup>3</sup> and Directive (EU)	(3)  Regulation (EU) 2016/679 of the European Parliament and of the Council <sup>3</sup> and Directive (EU)	

<sup>2</sup> Regulation (EC) No 45/2001 of the European Parliament and the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p.1).

<sup>3</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88.

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
2016/680 of the European Parliament and of the Council <sup>4</sup> were adopted on 27 April 2016. While the Regulation lays down general rules to protect natural persons in relation to the processing of personal data and to ensure the free movement of personal data within the Union, the Directive lays down the specific rules to protect natural persons in relation to the processing of personal data and to ensure the free movement of personal data within the Union in the fields of judicial cooperation in criminal matters and police cooperation.	2016/680 of the European Parliament and of the Council <sup>4</sup> were adopted on 27 April 2016. While the Regulation lays down general rules to protect natural persons in relation to the processing of personal data and to ensure the free movement of personal data within the Union, the Directive lays down the specific rules to protect natural persons in relation to the processing of personal data and to ensure the free movement of personal data within the Union in the fields of judicial cooperation in criminal matters and police cooperation..	2016/680 of the European Parliament and of the Council <sup>4</sup> were adopted on 27 April 2016. While the Regulation lays down general rules to protect natural persons in relation to the processing of personal data and to ensure the free movement of personal data within the Union, the Directive lays down the specific rules to protect natural persons in relation to the processing of personal data and to ensure the free movement of personal data within the Union in the fields of judicial cooperation in criminal matters and police cooperation.	
(4)  Regulation (EU) 2016/679 stresses the need for the necessary adaptations of Regulation (EC) No 45/2001 in order to provide a strong and coherent data protection framework in the Union and to allow application at the same time	(4)  Regulation (EU) 2016/679 stresses the need for the necessary adaptations of Regulation (EC) No 45/2001 in order to provide a strong and coherent data protection framework in the Union and to allow application at the same time	(4)  Regulation (EU) 2016/679 stresses the need for the necessary adaptations of Regulation (EC) No 45/2001 in order to provide a strong and coherent data protection framework in the Union and to allow application at the same time	

<sup>4</sup> Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131.

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
as Regulation (EU) 2016/679.	as Regulation (EU) 2016/679.	as Regulation (EU) 2016/679.	
<p>5)</p> <p>It is in the interest of a coherent approach to personal data protection throughout the Union, and of the free movement of personal data within the Union, to align as far as possible the data protection rules for Union institutions and bodies with the data protection rules adopted for the public sector in the Member States. Whenever the provisions of this Regulation are based on the same concept as the provisions of Regulation (EU) 2016/679, those two provisions should be interpreted homogeneously, in particular because the scheme of this Regulation should be understood as equivalent to the scheme of Regulation (EU) 2016/679.</p>	<p><b>AM 2</b></p> <p>(5)</p> <p>It is in the interest of a coherent approach to personal data protection throughout the Union, and of the free movement of personal data within the Union, to align <del>as far as possible</del> the data protection rules for Union institutions, <del>and bodies</del> <b>bodies, offices and agencies</b> with the data protection rules adopted for the public sector in the Member States. Whenever the provisions of this Regulation are based on the same concept as the provisions of Regulation (EU) 2016/679, those two provisions should <b><i>under the case law of the Court of Justice of the European Union<sup>1a</sup></i></b>, be interpreted homogeneously, in particular because the scheme of this Regulation should be understood as equivalent to the scheme of Regulation (EU) 2016/679.</p> <p><i><sup>1a</sup> Judgment of the Court of Justice of 9 March 2010, Commission v Germany, C-518/07, ECLI:EU:C:2010:125,</i></p>	<p>(5)</p> <p>It is in the interest of a coherent approach to personal data protection throughout the Union, and of the free movement of personal data within the Union, to align as far as possible the data protection rules for Union institutions and bodies with the data protection rules adopted for the public sector in the Member States. Whenever the provisions of this Regulation are based on the same concept as the provisions of Regulation (EU) 2016/679, those two provisions should be interpreted homogeneously, in particular because the scheme of this Regulation should be understood as equivalent to the scheme of Regulation (EU) 2016/679.</p>	<p>(5) It is in the interest of a coherent approach to personal data protection throughout the Union, and of the free movement of personal data within the Union, to align as far as possible the data protection rules for Union institutions, bodies, offices and agencies with the data protection rules adopted for the public sector in the Member States. Whenever the provisions of this Regulation are based on the same concept as the provisions of Regulation (EU) 2016/679, those two provisions should under the case law of the Court of Justice of the European Union, be interpreted homogeneously, in particular because the scheme of this Regulation should be understood as equivalent to the scheme of Regulation (EU) 2016/679.</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>paragraphs 26 and 28.</i>		
<p>(6)</p> <p>Persons whose personal data are processed by Union institutions and bodies in any context whatsoever, for example, because they are employed by those institutions and bodies should be protected. This Regulation should not apply to the processing of personal data of deceased persons. This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.</p>	<p>(6)</p> <p>Persons whose personal data are processed by Union institutions and bodies in any context whatsoever, for example, because they are employed by those institutions and bodies should be protected. This Regulation should not apply to the processing of personal data of deceased persons. This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.</p>	<p>(6)</p> <p>Persons whose personal data are processed by Union institutions and bodies in any context whatsoever, for example, because they are employed by those institutions and bodies should be protected. This Regulation should not apply to the processing of personal data of deceased persons. This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.</p>	
<p>(7)</p> <p>In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural</p>	<p>(7)</p> <p>In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural</p>	<p>(7)</p> <p>In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation.	persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation.	natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation.	
	<p><b>AM 3</b></p> <p><b>(7a)</b></p> <p><i>The data protection legal framework for the processing of data in the course of activities of Union institutions and bodies in the areas of freedom, security and justice and of the common foreign and security policy remains fragmented and creates legal uncertainty. This Regulation should therefore provide for harmonised rules for the protection and the free movement of personal data processed by Union institutions and bodies carrying out</i></p>	<p><b>(7a)</b></p> <p><b>This Regulation should apply to the processing of personal data by all Union institutions, bodies, offices and agencies. It should apply to the processing of personal data, wholly or partially by automated means, and to the processing otherwise than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. However, where other legal acts of the European Union provide for specific rules on the processing of personal data by Union</b></p>	<p><b>(7a)</b> This Regulation should apply to the processing of personal data by all Union institutions, bodies, offices and agencies. It should apply to the processing of personal data, wholly or partially by automated means, and to the processing otherwise than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.</p>



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>activities which fall within the scope of Chapters 4 and 5 of Title V of Part Three TFEU and Chapter 2 of Title V TEU.</i>	<b>institutions and bodies, these rules should remain unaffected by this Regulation.</b>	
<p>(8)</p> <p>In Declaration No 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, annexed to the final act of the intergovernmental conference which adopted the Treaty of Lisbon, the conference acknowledged that specific rules on the protection of personal data and the free movement of personal data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 TFEU could prove necessary because of the specific nature of those fields. This Regulation should therefore apply to Union agencies carrying out activities in the fields of judicial cooperation in criminal matters and police cooperation only to the extent that Union law applicable to such agencies does not</p>	<p><b>AM 4</b></p> <p>(8)</p> <p>In Declaration No 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, annexed to the final act of the intergovernmental conference which adopted the Treaty of Lisbon, the conference acknowledged that specific rules on the protection of personal data and the free movement of personal data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 TFEU could prove necessary because of the specific nature of those fields. <del>This Regulation should therefore apply to Union agencies carrying out activities in the fields of judicial cooperation in criminal matters and police cooperation only</del></p>	<p>(8)</p> <p>In Declaration No 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, annexed to the final act of the intergovernmental conference which adopted the Treaty of Lisbon, the conference acknowledged that specific rules on the protection of personal data and the free movement of personal data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 TFEU could prove necessary because of the specific nature of those fields. This Regulation should therefore <b>not apply to the processing of operational personal data, such as personal data processed for criminal investigation purposes by Union bodies, offices or agencies</b></p>	<p>(8) In Declaration No 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, annexed to the final act of the intergovernmental conference which adopted the Treaty of Lisbon, the conference acknowledged that specific rules on the protection of personal data and the free movement of personal data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 TFEU could prove necessary because of the specific nature of those fields. A separate Chapter of this Regulation containing general rules should therefore apply to the processing of operational personal data, such as personal data processed for criminal investigation purposes by Union bodies, offices or agencies carrying out activities in the fields</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
contain specific rules on the processing of personal data.	<p><del>to the extent that Union law applicable to such agencies does not contain specific rules on the processing of personal data.</del></p> <p><i>Furthermore, the common foreign and security policy has a specific nature and specific rules on the protection of personal data and it could prove necessary to ensure the free movement of personal data in that field also. It is therefore appropriate to regulate the processing of operational personal data by Union agencies established on the basis of Chapters 4 and 5 of Title V of Part Three TFEU and by missions referred to in Article 42(1) and Articles 43 and 44 TEU by establishing specific rules that derogate from a number of general rules laid down in this Regulation.</i></p>	<p>carrying out activities <b>which fall within the scope of Chapters 4 and 5 of Title V of Part Three of the TFEU</b> where the acts establishing these bodies, offices or agencies provide for comprehensive data protection rules applicable to the processing of such data, such as the acts establishing Europol and Eurojust [and the European Public Prosecutor's Office]. <del>in the fields of judicial cooperation in criminal matters and police cooperation only to the extent that Union law applicable to such agencies does not contain specific rules on the processing of personal data.</del> Processing of administrative personal data by those bodies, offices or agencies, such as staff data, should be covered by this Regulation.</p>	of judicial cooperation and criminal matters and police cooperation.
			(8-a) Directive (EU) 2016/680 provides harmonised rules for the protection and the free movement of personal data processed for the purposes of the prevention, investigation, detection or prosecution of criminal offences

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			or execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. In order to foster the same level of protection for natural persons through legally enforceable rights throughout the Union and to prevent divergences hampering the exchange of personal data between Union bodies, offices or agencies carrying out activities which fall within the scope of Chapters 4 and 5 of Title V of Part Three of the TFEU and competent authorities in Member States, the rules for the protection and the free movement of operational personal data processed by such Union bodies, offices or agencies should be consistent with Directive (EU) 2016/680.
			(8-aa) The general rules of the separate Chapter of this Regulation on the processing of operational personal data should apply without prejudice to the specific rules applicable to the processing of operational personal data by Union bodies, offices and

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			<p>agencies when carrying out activities falling within the scope of Chapters 4 and 5 of Title V of Part Three of the TFEU. Such specific rules should be regarded as <i>lex specialis</i> to the provisions in the separate Chapter of this Regulation on the processing of operational personal data (<i>lex specialis derogat legi generali</i>).</p> <p>In order to foster the removal of legal fragmentation, specific data protection rules applicable to the processing of operational personal data by Union bodies, offices or agencies when carrying out activities falling within the scope of Chapters 4 and 5 of Title V of Part Three of the TFEU should be consistent with the principles underpinning the separate Chapter of this Regulation on the processing of operational personal data, as well as with the provisions of this Regulation relating to independent supervision, remedies, liability and penalties.</p>
			(8a) The separate Chapter of this Regulation on the processing of

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			operational personal data <del>by</del> should apply to Union bodies, offices or agencies when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU, whether they exercise such activities as their main or ancillary tasks, for the purposes of prevention, detection, investigation or prosecution of criminal offences. However, it should not apply to Europol and the European Public Prosecutor's Office until the acts establishing Europol and the European Public Prosecutor's Office are amended with a view to rendering the separate Chapter of this Regulation on the processing of operational personal data, as revised, applicable to them.
			(8aa) The Commission should conduct a review of this Regulation, in particular the separate Chapter of this Regulation on the processing of operational personal data. The Commission should also conduct a review of other legal acts

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			<p>adopted on the basis of the Treaties which regulate the processing of operational personal data by Union bodies, offices or agencies when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU. After such a review, in order to ensure uniform and consistent protection of natural persons with regard to processing, the Commission may, submit, with a view to applying the separate Chapter on the processing of operational personal data to Europol and to European Public Prosecutor's Office, appropriate legislative proposals, including adaptations of the separate Chapter of this Regulation on the processing of operational personal data, if necessary. The adaptations should take into account <i>inter alia</i>, provisions relating to independent supervision, remedies, liability and penalties.</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			(8b) Processing of administrative personal data, such as staff data by Union bodies, offices or agencies carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU should be covered by this Regulation.
<p>(9)</p> <p>Directive (EU) 2016/680 provides harmonised rules for the protection and the free movement of personal data processed for the purposes of the prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. In order to foster the same level of protection for natural persons through legally enforceable rights throughout the Union and to prevent divergences hampering the exchange of personal data between Union agencies carrying out activities in the fields of judicial cooperation in criminal matters and police cooperation and competent</p>	<p>(9)</p> <p>Directive (EU) 2016/680 provides harmonised rules for the protection and the free movement of personal data processed for the purposes of the prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. In order to foster the same level of protection for natural persons through legally enforceable rights throughout the Union and to prevent divergences hampering the exchange of personal data between Union agencies carrying out activities in the fields of judicial cooperation in criminal matters and police cooperation and competent</p>	<p>(9)</p> <p>Directive (EU) 2016/680 provides harmonised rules for the protection and the free movement of personal data processed for the purposes of the prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. In order to foster the same level of protection for natural persons through legally enforceable rights throughout the Union and to prevent divergences hampering the exchange of personal data between Union <b>bodies, offices or</b> agencies carrying out activities <b>which fall within the scope of Chapters 4</b></p>	Deletion

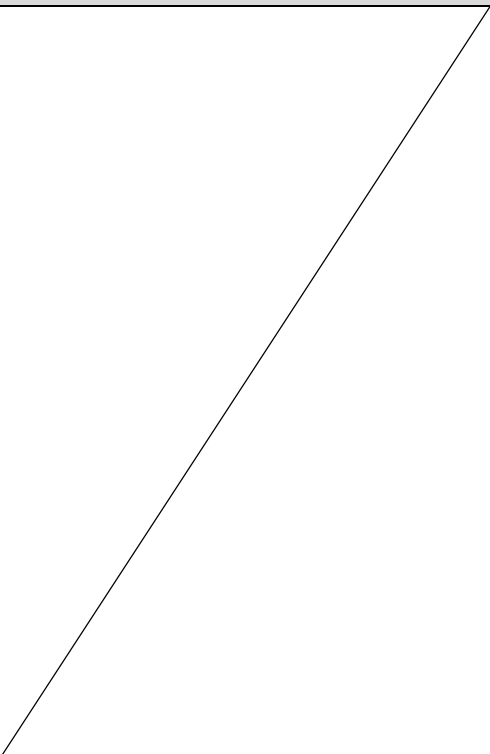
COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
authorities in Member States, the rules for the protection and the free movement of operational personal data processed by such Union agencies should draw on the principles underpinning this Regulation and be consistent with Directive (EU) 2016/680.	authorities in Member States, the rules for the protection and the free movement of operational personal data processed by such Union agencies should draw on the principles underpinning this Regulation and be consistent with Directive (EU) 2016/680.	<b>and 5 of Title V of Part Three of the TFEU in the fields of judicial cooperation in criminal matters and police cooperation</b> and competent authorities in Member States, the rules for the protection and the free movement of operational personal data processed by such Union <b>bodies, offices or</b> agencies should <del>draw on the principles underpinning this Regulation and</del> be consistent with Directive (EU) 2016/680.	



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>(10)</p> <p>Where the founding act of a Union agency carrying out activities which fall within the scope of Chapters 4 and 5 of Title V of the Treaty lays down a standalone data protection regime for the processing of operational personal data such regimes should be unaffected by this Regulation. However, the Commission should, in accordance with Article 62 of Directive (EU) 2016/680, by 6 May 2019 review Union acts which regulate processing by the competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and, where appropriate, make the necessary proposals to amend those acts to ensure a consistent approach to the protection of personal data in the area of judicial cooperation in criminal matters and police</p>	<p>(10)</p> <p>Where the founding act of a Union agency carrying out activities which fall within the scope of Chapters 4 and 5 of Title V of the Treaty lays down a standalone data protection regime for the processing of operational personal data such regimes should be unaffected by this Regulation. However, the Commission should, in accordance with Article 62 of Directive (EU) 2016/680, by 6 May 2019 review Union acts which regulate processing by the competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and, where appropriate, make the necessary proposals to amend those acts to ensure a consistent approach to the protection of personal data in the area of judicial cooperation in criminal matters and police</p>	<p><del>(10)</del></p> <p><del>Where the founding act of a Union agency carrying out activities which fall within the scope of Chapters 4 and 5 of Title V of the Treaty lays down a standalone data protection regime for the processing of operational personal data such regimes should be unaffected by this Regulation. However, the Commission should, in accordance with Article 62 of Directive (EU) 2016/680, by 6 May 2019 review Union acts which regulate processing by the competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and, where appropriate, make the necessary proposals to amend those acts to ensure a consistent approach to the protection of personal data in the</del></p>	<p>deletion</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
cooperation.	cooperation.	<del>area of judicial cooperation in criminal matters and police cooperation.</del>	
		<p><b>(10a)</b></p> <p><b>This Regulation should apply to the processing of personal data by Union institutions, bodies, offices or agencies carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU. This Regulation does not apply to the processing of personal data by missions referred to in Articles 42(1), and 43 and 44 of the TEU, which implement the common security and defence policy.</b></p>	<p>(10a) This Regulation should apply to the processing of personal data by Union institutions, bodies, offices or agencies carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU. This Regulation does not apply to the processing of personal data by missions referred to in Articles 42(1), 43 and 44 of the TEU, which implement the common security and defence policy. Where appropriate, relevant proposals should be put forward to further regulate the processing of personal data in the field of the common security and defence policy.</p>
		<p><b>Where appropriate, relevant proposals could be put forward to further regulate the processing of personal data in the field of the common security and defence policy.</b></p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>(11)</p> <p>The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.</p>	<p>(11)</p> <p>The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.</p>	<p>(11)</p> <p>The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.</p>	
<p>To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective</p>	<p>To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective</p>	<p>To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.</p>	<p>factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.</p>	<p>factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>(12)</p> <p>The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data protection obligations. The explicit introduction of ‘pseudonymisation’ in this Regulation is not intended to preclude any other measures of data protection.</p>	<p>(12)</p> <p>The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data protection obligations. The explicit introduction of ‘pseudonymisation’ in this Regulation is not intended to preclude any other measures of data protection.</p>	<p>(12)</p> <p>The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data protection obligations. The explicit introduction of ‘pseudonymisation’ in this Regulation is not intended to preclude any other measures of data protection.</p>	
<p>(13)</p> <p>Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.</p>	<p>(13)</p> <p>Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.</p>	<p>(13)</p> <p>Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
		identify them.	
<p>(14)</p> <p>Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is</p>	<p><b>AM 5</b></p> <p>(14)</p> <p>Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes,</p>	<p>(14)</p> <p>Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data</p>	<p>(14) Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.	consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided. <i>At the same time, the data subject should have the right to withdraw consent at any time without affecting the lawfulness of processing based on consent before its withdrawal.</i>	subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided. <b>In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have an opportunity to give their consent only to certain areas of research or parts of</b>	following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided. At the same time, the data subject should have the right to withdraw consent at any time without affecting the lawfulness of processing based on consent before its withdrawal. In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research.

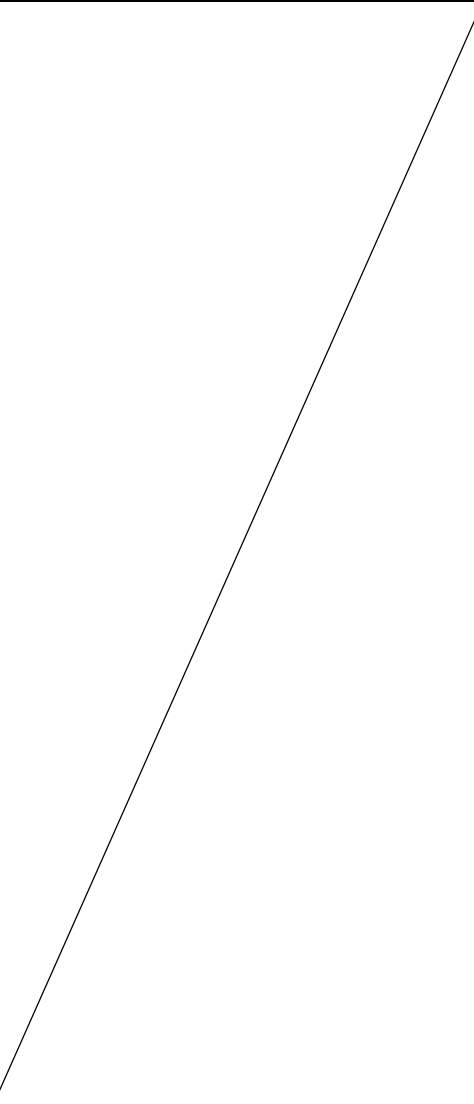
COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
		<b>research projects to the extent allowed by the intended purpose.</b>	Data subjects should have an opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.
<p>(15)</p> <p>Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural</p>	<p><b>AM 6</b></p> <p>(15)</p> <p>Any processing of personal data should be lawful and fair <i><b>and done for clear and well-defined purposes</b></i>. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of</p>	<p>(15)</p> <p>Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural</p>	<p>(15) Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned</p>



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a</p>	<p>the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not</p>	<p>persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for</p>	<p>and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.	kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to, <b><i>disclosure during the transmission of,</i></b> or use of personal data and the equipment used for the processing.	erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.	be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to, disclosure during the transmission of, or use of personal data and the equipment used for the processing.
(16)  In accordance with the principle of accountability, where Union institutions and bodies transmit personal data within or to other Union institutions or bodies, they should verify whether such personal data is required for the legitimate performance of tasks covered by the competence of the recipient where the recipient is not part of the controller. In particular, following a recipient's request for transmission	(16)  In accordance with the principle of accountability, where Union institutions and bodies transmit personal data within or to other Union institutions or bodies, they should verify whether such personal data is required for the legitimate performance of tasks covered by the competence of the recipient where the recipient is not part of the controller. In particular, following a recipient's request for transmission	(16)  In accordance with the principle of accountability, where Union institutions and bodies transmit personal data within or to other Union institutions or bodies, they should verify whether such personal data is required for the legitimate performance of tasks covered by the competence of the recipient where the recipient is not part of the controller. In particular, following a recipient's request for	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
of personal data, the controller should verify the existence of a relevant ground of its lawful processing of personal data, the competence of the recipient and should make a provisional evaluation of the necessity for the transmission of the data. If doubts arise as to this necessity, the controller should seek further information from the recipient. The recipient should ensure that the necessity for the transmission of the data can be subsequently verified.	of personal data, the controller should verify the existence of a relevant ground of its lawful processing of personal data, the competence of the recipient and should make a provisional evaluation of the necessity for the transmission of the data. If doubts arise as to this necessity, the controller should seek further information from the recipient. The recipient should ensure that the necessity for the transmission of the data can be subsequently verified.	transmission of personal data, the controller should verify the existence of a relevant ground of its lawful processing of personal data, the competence of the recipient and should make a provisional evaluation of the necessity for the transmission of the data. If doubts arise as to this necessity, the controller should seek further information from the recipient. The recipient should ensure that the necessity for the transmission of the data can be subsequently verified.	
(17)  In order for processing to be lawful, personal data should be processed on the basis of the necessity of performance of a task carried out in the public interest by Union institutions and bodies or in the exercise of their official authority, the necessity for compliance with the legal obligation to which the controller is subject or some other legitimate basis as referred to in this Regulation, including the consent of	(17)  In order for processing to be lawful, personal data should be processed on the basis of the necessity of performance of a task carried out in the public interest by Union institutions and bodies or in the exercise of their official authority, the necessity for compliance with the legal obligation to which the controller is subject or some other legitimate basis as referred to in this Regulation, including the consent of	(17)  In order for processing to be lawful, personal data should be processed on the basis of the necessity of performance of a task carried out in the public interest by Union institutions and bodies or in the exercise of their official authority, the necessity for compliance with the legal obligation to which the controller is subject or some other legitimate basis as referred to in this	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>the data subject concerned or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. Processing of personal data for the performance of tasks carried out in the public interest by the Union institutions and bodies includes the processing of personal data necessary for the management and functioning of those institutions and bodies. The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian</p>	<p>the data subject concerned or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. Processing of personal data for the performance of tasks carried out in the public interest by the Union institutions and bodies includes the processing of personal data necessary for the management and functioning of those institutions and bodies. The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian</p>	<p>Regulation, including the consent of the data subject concerned or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. Processing of personal data for the performance of tasks carried out in the public interest by the Union institutions and bodies includes the processing of personal data necessary for the management and functioning of those institutions and bodies. The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.	purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.	instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.	
(18)  The Union law including the internal rules referred to in this Regulation should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union and the European Court of Human Rights.	<b>AM 7</b>  (18)  The Union law <del>including the internal rules</del> referred to in this Regulation should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the <del>requirements case-law of the Court of Justice of the European Union set out in the Charter and</del> Court of the European <i>Convention for the Protection of Human Rights and Fundamental Freedoms.</i>	(18)  The Union law <del>including the internal rules</del> referred to in this Regulation should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the <b>requirements set out in the Charter and the European Convention for the Protection of Human Rights and Fundamental Freedoms. case-law of the Court of Justice of the European Union and the European Court of Human Rights.</b>	(18) The Union law referred to in this Regulation should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the requirements set out in the Charter and the European Convention for the Protection of Human Rights and Fundamental Freedoms.
		(18a)  <b>The internal rules referred to in this Regulation should be clear</b>	Council suggestion:  (18a)

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
		<p><b>and precise acts of general application intended to produce legal effects vis-à-vis data subjects, adopted at the highest level of management of the Union institutions and bodies within their competencies and in matters relating to their operation and should be published in the Official Journal of the European Union. The application of these rules should be foreseeable to persons subject to them in accordance with the requirements set out in the Charter and the European Convention for the Protection of Human Rights and Freedoms. Internal rules may take the form of decisions, in particular when adopted by Union institutions.</b></p>	<p>The internal rules referred to in this Regulation should be clear and precise acts of general application intended to produce legal effects vis-à-vis data subjects, adopted at the highest level of management of the Union institutions and bodies within their competencies and in matters relating to their operation and should be published in the Official Journal of the European Union. The application of these rules should be foreseeable to persons subject to them in accordance with the requirements set out in the Charter and the European Convention for the Protection of Human Rights and Freedoms. Internal rules may take the form of decisions, in particular when adopted by Union institutions.</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>(19) The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. The legal basis provided by Union law for the processing of personal data may also provide a legal basis for further processing. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.</p>	<p>(19)The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. The legal basis provided by Union law for the processing of personal data may also provide a legal basis for further processing. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.</p>	<p>(19)The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. The legal basis provided by Union law for the processing of personal data may also provide a legal basis for further processing. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.</p>	
8394/1/18 REV 1		CHS/np	38

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>(20)</p> <p>Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC<sup>5</sup> a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or</p>	<p><b>AM 8</b></p> <p>(20)</p> <p>Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC<sup>5</sup> a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller <b>and</b>, the purposes of the processing for which the personal data are intended <b>and the categories of recipients of the data, and be</b></p>	<p>(20)</p> <p>Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC<sup>5</sup> a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no</p>	<p>(20) Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC<sup>5</sup> a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has</p>

<sup>5</sup> Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ J 95, 21.4.1993, p.29).



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
withdraw consent without detriment.	<i>informed on the right of access and of intervention in respect of the data.</i> Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.	genuine or free choice or is unable to refuse or withdraw consent without detriment.	no genuine or free choice or is unable to refuse or withdraw consent without detriment.
<p>(21)</p> <p>Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to creating personality profiles and the collection of personal data with regard to children when using services offered directly to a child on websites of Union institutions and bodies, such as interpersonal communication services or online selling of tickets and when the processing of personal data is based on consent.</p>	<p>(21)</p> <p>Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to creating personality profiles and the collection of personal data with regard to children when using services offered directly to a child on websites of Union institutions and bodies, such as interpersonal communication services or online selling of tickets and when the processing of personal data is based on consent.</p>	<p>(21)</p> <p>Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to creating personality profiles and the collection of personal data with regard to children when using services offered directly to a child on websites of Union institutions and bodies, such as interpersonal communication services or online selling of tickets and when the processing of personal data is based on consent.</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>(22) those recipients demonstrate that the transmission is necessary for the attainment of their objective, is proportionate and does not go beyond what is necessary to attain that objective. Union institutions and bodies should demonstrate such necessity when they themselves initiate the transmission, in compliance with the principle of transparency.</p>	<p><b>AM 9</b></p> <p>(22)</p> <p>When recipients established in the Union and subject to Regulation (EU) 2016/679 or Directive (EU) 2016/680, would like to have personal data transmitted to them by Union institutions and bodies, those recipients <del>demonstrate that the</del> <b>should provide the controller with a reasoned request for transmission which should serve as a basis for the controller to assess whether that</b> transmission is necessary for the attainment of their objective, is proportionate and does not go beyond what is necessary to attain that objective. Union institutions and bodies should demonstrate such necessity when they themselves initiate the transmission, in compliance with the principle of transparency</p>	<p>(22)</p> <p>When recipients <b>other than Union institutions and bodies</b> established in the Union <del>and subject to Regulation (EU) 2016/679 or Directive (EU) 2016/680</del>, would like to have personal data transmitted to them by Union institutions and bodies, those recipients should demonstrate <b>either that the data are necessary for the performance of their task carried out in the public interest or in the exercise of official authority vested in them, or that it is necessary to have the data transmitted that the transmission is necessary</b> for the attainment of their objective, <b>and that it is</b> proportionate and does not go beyond what is necessary to attain that objective. Union institutions and bodies should demonstrate such necessity when they themselves initiate the transmission, in compliance with the principle of transparency. <b>The requirements laid down in this</b></p>	<p>Council suggestion:</p> <p>(22)When recipients other than Union institutions and bodies established in the Union would like to have personal data transmitted to them by Union institutions and bodies, those recipients should demonstrate that it is necessary to have the data transmitted to these recipients either for the performance of their task carried out in the public interest or in the exercise of official authority vested in them. Alternatively, those recipients should demonstrate that the transmission is necessary for a specific purpose in the public interest and the controller should establish whether there is any reason to assume that the data subject's legitimate interests might be prejudiced, in which case the controller should demonstrably weigh the various competing interests in order to assess the proportionality of the requested</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
		<b>Regulation for transmissions to recipients other than Union institutions and bodies established in the Union should be understood as supplementary to the conditions for lawful processing, such as an appropriate legal basis and compliance with the principles relating to the processing of personal data.</b>	transmission of personal data. Those specific purposes could relate to transparency of Union institutions and bodies. Furthermore, Union institutions and bodies should demonstrate such necessity when they themselves initiate the transmission, in compliance with the principle of transparency and good administration. The requirements laid down in this Regulation for transmissions to recipients other than Union institutions and bodies established in the Union should be understood as supplementary to the conditions for lawful processing.
(23)  Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms.	<b>AM 10</b>  (23)  Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing	(23)  Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms.	(23) Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Such personal data should not be processed unless

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term ‘racial origin’ in this Regulation does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races. The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. In addition to the specific requirements for processing of sensitive data, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing such special categories of personal data should be explicitly provided, inter alia, where the data subject gives his or her explicit consent or in respect of specific	could create significant risks to the fundamental rights and freedoms. <b><i>Such personal data should not be processed unless processing is allowed in specific cases set out in this Regulation.</i></b> Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term ‘racial origin’ in this Regulation does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races. The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. In addition to the specific requirements for processing of sensitive data, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for	Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term ‘racial origin’ in this Regulation does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races. The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. In addition to the specific requirements for processing of sensitive data, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing such special categories of personal data should be explicitly provided, inter alia, where the data subject gives his or	specific conditions set out in this Regulation are met. Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term ‘racial origin’ in this Regulation does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races. The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. In addition to the specific requirements for processing of sensitive data, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing such

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
needs in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.	processing such special categories of personal data should be explicitly provided, inter alia, where the data subject gives his or her explicit consent or in respect of specific needs in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.	her explicit consent or in respect of specific needs in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.	special categories of personal data should be explicitly provided, inter alia, where the data subject gives his or her explicit consent or in respect of specific needs in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<p>AM 11</p> <p>(23a)</p> <p><i>Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems. Therefore, this Regulation should provide for harmonised conditions for the processing of special categories of personal data concerning health, in respect of specific needs, in particular where the processing of such data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy. Union law should provide for specific and suitable measures so as to protect the fundamental rights and the personal data of natural persons.</i></p>		<p>(23a) Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems. Therefore, this Regulation should provide for harmonised conditions for the processing of special categories of personal data concerning health, in respect of specific needs, in particular where the processing of such data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy. Union law should provide for specific and suitable measures so as to protect the fundamental rights and the personal data of natural persons.</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>(24)</p> <p>The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons. In that context, ‘public health’ should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council<sup>6</sup>, namely all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of data concerning health for reasons of</p>	<p><b>AM 12</b></p> <p>(24)</p> <p>The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons. In that context, ‘public health’ should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council<sup>6</sup>, namely all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of</p>	<p>(24)</p> <p>The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons. In that context, ‘public health’ should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council<sup>6</sup>, namely all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of data concerning</p>	<p>(24) The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons. In that context, ‘public health’ should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council<sup>6</sup>, namely all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of data concerning health for reasons of public interest should not result in</p>

<sup>6</sup> Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work ([OJ L 354, 31.12.2008, p. 70](#)).

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
public interest should not result in personal data being processed for other purposes by third parties.	mortality. Such processing of data concerning health for reasons of public interest should not result in personal data being processed for other purposes <del>by third parties.</del>	health for reasons of public interest should not result in personal data being processed for other purposes by third parties.	personal data being processed for other purposes.
<p>(25)</p> <p>If the personal data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights. Identification should include the digital identification of a data subject, for example through authentication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data</p>	<p>(25)</p> <p>If the personal data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights. Identification should include the digital identification of a data subject, for example through authentication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data</p>	<p>(25)</p> <p>If the personal data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights. Identification should include the digital identification of a data subject, for example through authentication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data</p>	



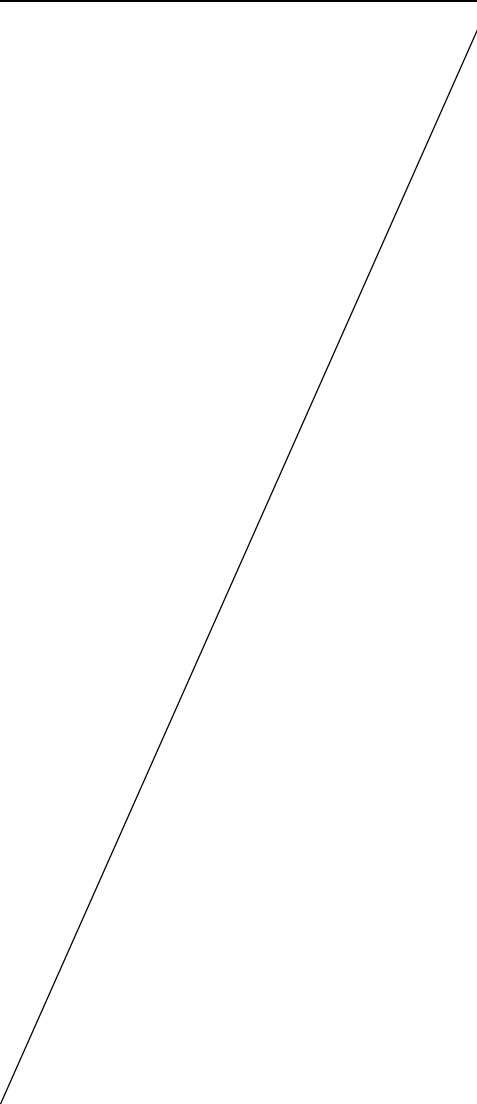
COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
controller.	controller.	controller.	
<p>(26)</p> <p>The processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be subject to appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation. Those safeguards should ensure that technical and organisational measures are in place in order to ensure, in particular, the principle of data minimisation. The further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is to be carried out when the controller has assessed the feasibility to fulfil those purposes by processing data which do not permit or no longer permit the identification of data subjects, provided that appropriate safeguards exist (such as, for instance, pseudonymisation of the data).</p>	<p>(26)</p> <p>The processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be subject to appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation. Those safeguards should ensure that technical and organisational measures are in place in order to ensure, in particular, the principle of data minimisation. The further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is to be carried out when the controller has assessed the feasibility to fulfil those purposes by processing data which do not permit or no longer permit the identification of data subjects, provided that appropriate safeguards exist (such as, for instance, pseudonymisation of the data).</p>	<p>(26)</p> <p>The processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be subject to appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation. Those safeguards should ensure that technical and organisational measures are in place in order to ensure, in particular, the principle of data minimisation. The further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is to be carried out when the controller has assessed the feasibility to fulfil those purposes by processing data which do not permit or no longer permit the identification of data subjects,</p>	<p>Council suggestion:</p> <p>(26)</p> <p>The processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be subject to appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation. Those safeguards should ensure that technical and organisational measures are in place in order to ensure, in particular, the principle of data minimisation. The further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is to be carried out when the controller has assessed the feasibility to fulfil those purposes by processing data which do not permit or no longer permit the identification of data subjects,</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
Union institutions and bodies should provide for appropriate safeguards for the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in Union law, which may include internal rules.	Union institutions and bodies should provide for appropriate safeguards for the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in Union law, <del>which may include internal rules.</del>	data). Union institutions and bodies should provide for appropriate safeguards for the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in Union law, which may include internal rules <b>adopted by Union institutions and bodies in matters relating to their operation.</b>	provided that appropriate safeguards exist (such as, for instance, pseudonymisation of the data). Union institutions and bodies should provide for appropriate safeguards for the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in Union law, which may include internal rules adopted by Union institutions and bodies in matters relating to their operation.
(27)  Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. The controller should also provide means for requests to be made electronically, especially where personal data are	(27)  Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. The controller should also provide means for requests to be made electronically, especially where personal data are	(27)  Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. The controller should also provide means for requests to be made electronically, especially where	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
processed by electronic means. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests.	processed by electronic means. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests.	personal data are processed by electronic means. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests.	
(28)  The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling. Where the personal data are collected from the data subject, the data subject should also be informed	(28)  The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling. Where the personal data are collected from the data subject, the data subject should also be informed	(28)  The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling. Where the personal data are collected from the data subject, the	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
whether he or she is obliged to provide the personal data and of the consequences, where he or she does not provide such data. That information may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing. Where the icons are presented electronically, they should be machine-readable.	whether he or she is obliged to provide the personal data and of the consequences, where he or she does not provide such data. That information may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing. Where the icons are presented electronically, they should be machine-readable.	data subject should also be informed whether he or she is obliged to provide the personal data and of the consequences, where he or she does not provide such data. That information may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing. Where the icons are presented electronically, they should be machine-readable.	
(29)  The information in relation to the processing of personal data relating to the data subject should be given to him or her at the time of collection from the data subject, or, where the personal data are obtained from another source, within a reasonable period, depending on the circumstances of the case. Where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal data are first	(29)  The information in relation to the processing of personal data relating to the data subject should be given to him or her at the time of collection from the data subject, or, where the personal data are obtained from another source, within a reasonable period, depending on the circumstances of the case. Where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal data are first	(29)  The information in relation to the processing of personal data relating to the data subject should be given to him or her at the time of collection from the data subject, or, where the personal data are obtained from another source, within a reasonable period, depending on the circumstances of the case. Where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>disclosed to the recipient.</p> <p>Where the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information. Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided.</p>	<p>disclosed to the recipient.</p> <p>Where the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information. Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided.</p>	<p>data are first disclosed to the recipient.</p> <p>Where the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information. Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided.</p>	
<p>(30)</p> <p>A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing</p>	<p>(30)</p> <p>A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing</p>	<p>(30)</p> <p>A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. This includes the right for data subjects to have access to data concerning their health, for example the data in</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided. Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject. Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data</p>	<p>information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided. Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject. Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data</p>	<p>their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided. Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject. Where the controller processes a large quantity of information concerning the data subject, the</p>	

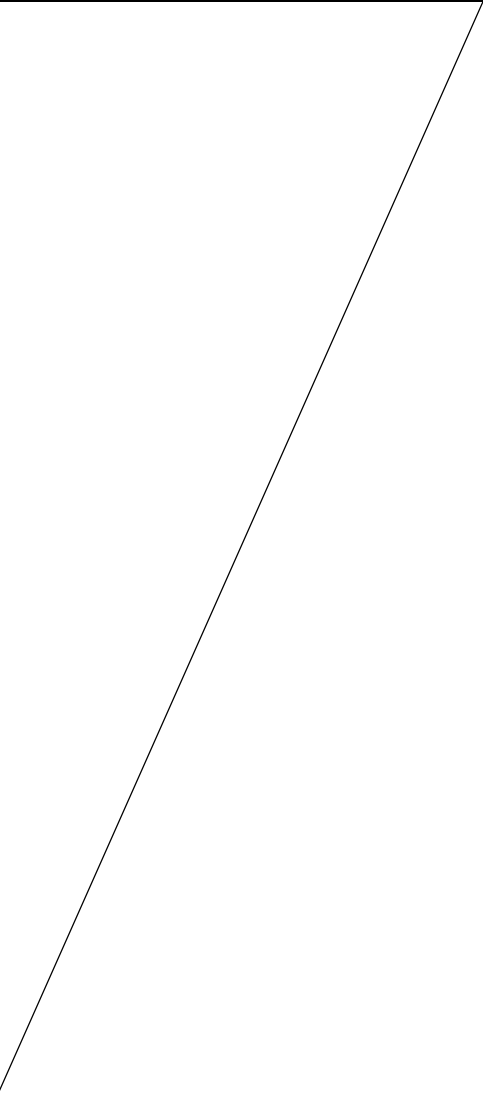
COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
subject specify the information or processing activities to which the request relates.	subject specify the information or processing activities to which the request relates.	controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.	
<p>(31)</p> <p>A data subject should have the right to have personal data concerning him or her rectified and a ‘right to be forgotten’ where the retention of such data infringes this Regulation or Union law to which the controller is subject. A data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. That right is relevant in particular where the data</p>	<p>(31)</p> <p>A data subject should have the right to have personal data concerning him or her rectified and a ‘right to be forgotten’ where the retention of such data infringes this Regulation or Union law to which the controller is subject. A data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. That right is relevant in particular where the data</p>	<p>(31)</p> <p>A data subject should have the right to have personal data concerning him or her rectified and a ‘right to be forgotten’ where the retention of such data infringes this Regulation or Union law to which the controller is subject. A data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. That</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.	subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.	right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.	
(32)	(32)	(32)	



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
To strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data. In doing so, that controller should take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform the controllers which are processing the personal data of the data subject's request.	To strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data. In doing so, that controller should take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform the controllers which are processing the personal data of the data subject's request.	To strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data. In doing so, that controller should take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform the controllers which are processing the personal data of the data subject's request.	
(33)  Methods by which to restrict the processing of personal data could include, inter alia, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website. In	(33)  Methods by which to restrict the processing of personal data could include, inter alia, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website. In	(33)  Methods by which to restrict the processing of personal data could include, inter alia, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website. In	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be clearly indicated in the system.	automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be clearly indicated in the system.	automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be clearly indicated in the system.	
(34)  To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller. Data controllers should be encouraged to develop interoperable formats that enable data portability. That right should apply where the data subject provided the personal data on the	(34)  To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller. Data controllers should be encouraged to develop interoperable formats that enable data portability. That right should apply where the data subject provided the personal data on the	(34)  To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller. Data controllers should be encouraged to develop interoperable formats that enable data portability. That right should apply where the data subject	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>basis of his or her consent or the processing is necessary for the performance of a contract. It should therefore not apply where the processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller. The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible. Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation. Furthermore, that right should not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in this Regulation and should, in particular,</p>	<p>basis of his or her consent or the processing is necessary for the performance of a contract. It should therefore not apply where the processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller. The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible. Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation. Furthermore, that right should not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in this Regulation and should, in particular,</p>	<p>provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It should therefore not apply where the processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller. The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible. Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation. Furthermore, that right should not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract to the extent that and for as long as the personal data are necessary for the performance of that contract. Where technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another.	not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract to the extent that and for as long as the personal data are necessary for the performance of that contract. Where technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another.	that right as set out in this Regulation and should, in particular, not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract to the extent that and for as long as the personal data are necessary for the performance of that contract. Where technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another.	
(35)  Where personal data might lawfully be processed because processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation. It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the	(35)  Where personal data might lawfully be processed because processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation. It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the	(35)  Where personal data might lawfully be processed because processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation. It should be for the controller to demonstrate that its compelling legitimate interest	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
fundamental rights and freedoms of the data subject.	fundamental rights and freedoms of the data subject.	overrides the interests or the fundamental rights and freedoms of the data subject.	
<p>(36)</p> <p>The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as e-recruiting practices without any human intervention. Such processing includes ‘profiling’ that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or</p>	<p>(36)</p> <p>The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as e-recruiting practices without any human intervention. Such processing includes ‘profiling’ that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or</p>	<p>(36)</p> <p>The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as e-recruiting practices without any human intervention. Such processing includes ‘profiling’ that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
		legal effects concerning him or her or	
similarly significantly affects him or her. However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union law. In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child. In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors	similarly significantly affects him or her. However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union law. In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child. In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors	similarly significantly affects him or her. However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union law. In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child. In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions.	which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions.	organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions.	
(37)  Legal acts adopted on the basis of the Treaties or internal rules of Union institutions and bodies may impose restrictions concerning specific principles and the rights of	<b>AM 13</b>  (37)  Legal acts adopted on the basis of the Treaties <del>or internal rules of Union institutions and bodies</del> may impose	(37)  Legal acts adopted on the basis of the Treaties or internal rules <del>of</del> <b>adopted by</b> Union institutions and bodies <b>in matters relating to their operation</b> may impose restrictions	Council suggestion:  (37)  Legal acts adopted on the basis of the Treaties or internal rules adopted by Union institutions and

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
information, access to and rectification or erasure of personal data, the right to data portability, confidentiality of electronic communications as well as the communication of a personal data breach to a data subject and certain related obligations of the controllers, as far as necessary and proportionate in a democratic society to safeguard public security, the prevention, investigation and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, including the protection of human life especially in response to natural or manmade disasters, internal security of Union institutions and bodies, other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, the keeping of public registers kept for reasons of general public interest or the protection of the data subject or the rights and	restrictions concerning specific principles and the rights of information, access to and rectification or erasure of personal data, the right to data portability, confidentiality of electronic communications as well as the communication of a personal data breach to a data subject and certain related obligations of the controllers, as far as necessary and proportionate in a democratic society to safeguard public security, the prevention, investigation and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, including the protection of human life especially in response to natural or manmade disasters, internal security of Union institutions and bodies, other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, the keeping of public registers kept for reasons of general public interest or the protection of the data subject or the rights and	concerning specific principles and the rights of information, access to and rectification or erasure of personal data, the right to data portability, confidentiality of electronic communications <b>data</b> as well as the communication of a personal data breach to a data subject and certain related obligations of the controllers, as far as necessary and proportionate in a democratic society to safeguard public security, the prevention, investigation and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, including the protection of human life especially in response to natural or manmade disasters, internal security of Union institutions and bodies, other important objectives of general public interest of the Union or of a Member State, in particular <b>the objectives of the Common Foreign and Security Policy of the Union</b> or an important economic or financial interest of	bodies in matters relating to their operation may impose restrictions concerning specific principles and the rights of information, access to and rectification or erasure of personal data, right to data portability, confidentiality of electronic communications data as well as the communication of a personal data breach to a data subject and certain related obligations of the controllers, as far as necessary and proportionate in a democratic society to safeguard public security, the prevention, investigation and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, including the protection of human life especially in response to natural or manmade disasters, internal security of Union institutions and bodies, other important objectives of general public interest of the Union or of a Member State, in particular the objectives of the



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
freedoms of others, including social protection, public health and humanitarian purposes.	freedoms of others, including social protection, public health and humanitarian purposes.	the Union or of a Member State, the keeping of public registers kept for reasons of general public interest or the protection of the data subject or the rights and freedoms of others, including social protection, public health and humanitarian purposes.	Common Foreign and Security Policy of the Union or an important economic or financial interest of the Union or of a Member State, the keeping of public registers kept for reasons of general public interest or the protection of the data subject or the rights and freedoms of others, including social protection, public health and humanitarian purposes.
Where a restriction is not provided for in legal acts adopted on the basis of the Treaties or their internal rules, Union institutions and bodies may in a specific case impose an ad hoc restriction concerning specific principles and the rights of data subject if such a restriction respects the essence of the fundamental rights and freedoms and, in relation to a specific processing operation, is necessary and proportionate in a democratic society to safeguard one or more of the objectives mentioned in paragraph 1. The restriction should be notified to the data protection officer. All	<b>AM 14</b> <del>Where a restriction is not provided for in legal acts adopted on the basis of the Treaties or their internal rules, Union institutions and bodies may in a specific case impose an ad hoc restriction concerning specific principles and the rights of data subject if such a restriction respects the essence of the fundamental rights and freedoms and, in relation to a specific processing operation, is necessary and proportionate in a democratic society to safeguard one or more of the objectives mentioned in paragraph 1. The restriction should be notified to the data</del>	<del>Where a restriction is not provided for in legal acts adopted on the basis of the Treaties or their internal rules, Union institutions and bodies may in a specific case impose an ad hoc restriction concerning specific principles and the rights of data subject if such a restriction respects the essence of the fundamental rights and freedoms and, in relation to a specific processing operation, is necessary and proportionate in a democratic society to safeguard one or more of the objectives mentioned in paragraph 1. The restriction should be notified to</del>	deletion

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
restrictions should be in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.	<del>protection officer. All restrictions should be in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.</del>	<del>the data protection officer. All restrictions should be in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.</del>	
(38)  The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons. The risk to the rights and freedoms of natural persons, of varying likelihood and	(38)  The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons. The risk to the rights and freedoms of natural persons, of varying likelihood and	(38)  The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons. The risk to the rights and freedoms of natural persons, of varying likelihood and	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal	severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal	severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health,	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects. The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.	preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects. The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.	personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects. The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.	
(39)  The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the	(39)  The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the	(39)  The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.	requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.	to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.	
	<b>AM 15</b>  <b>(39a)</b>  <b>Regulation (EU) 2016/679 provides</b>		(39a) Regulation (EU) 2016/679 provides for controllers to demonstrate compliance by adherence to approved certification mechanisms.

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>for controllers to demonstrate compliance by adherence to approved certification mechanisms. Likewise, Union institutions and bodies should be able to demonstrate compliance with this Regulation by obtaining certification in accordance with Article 42 of Regulation (EU) 2016/679.</i>		Likewise, Union institutions and bodies should be able to demonstrate compliance with this Regulation by obtaining certification in accordance with Article 42 of Regulation (EU) 2016/679.
(40)  The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors requires a clear allocation of the responsibilities under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.	(40)  The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors requires a clear allocation of the responsibilities under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.	(40)  The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors requires a clear allocation of the responsibilities under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.	
(41)  To ensure compliance with the requirements of this Regulation in	(41)  To ensure compliance with the requirements of this Regulation in	(41)  To ensure compliance with the requirements of this Regulation in	(41) To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which meet the requirements of this Regulation, including for the security of processing. The adherence of processors other than Union institutions and bodies to an approved code of conduct or an approved certification mechanism can be used as an element to demonstrate compliance with the obligations of the controller. The carrying-out of processing by a processor should be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purposes of the processing, the type of	respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which meet the requirements of this Regulation, including for the security of processing. The adherence of processors other than Union institutions and bodies to an approved code of conduct or an approved certification mechanism can be used as an element to demonstrate compliance with the obligations of the controller. The carrying-out of processing by a processor should be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purposes of the processing, the type of	respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which meet the requirements of this Regulation, including for the security of processing. The adherence of processors other than Union institutions and bodies to an approved code of conduct or an approved certification mechanism can be used as an element to demonstrate compliance with the obligations of the controller. The carrying-out of processing by a processor <b>other than a Union institution or body</b> should be governed by a contract, or, <b>in case of Union institutions and bodies acting as processors, by a contract or</b> other legal act under Union <del>or Member State</del> law, binding the processor to the	processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which meet the requirements of this Regulation, including for the security of processing. The adherence of processors other than Union institutions and bodies to an approved code of conduct or an approved certification mechanism can be used as an element to demonstrate compliance with the obligations of the controller. The carrying-out of processing by a processor other than a Union institution or body should be governed by a contract, or, in case of Union institutions and bodies acting as processors, by a contract or other legal act under Union law, binding the processor to the controller, setting out the subject-matter and duration of the

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject. The controller and processor should be able to choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by the European Data Protection Supervisor and then adopted by the Commission. After the completion of the processing on behalf of the controller, the processor should, at the choice of the controller, return or delete the personal data, unless there is a requirement to store that personal data under Union or Member State law to which the processor is subject.</p>	<p>personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject. The controller and processor should be able to choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by the European Data Protection Supervisor and then adopted by the Commission. After the completion of the processing on behalf of the controller, the processor should, at the choice of the controller, return or delete the personal data, unless there is a requirement to store that personal data under Union or Member State law to which the processor is subject.</p>	<p>controller, setting out the subject-matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject. The controller and processor should be able to choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by the European Data Protection Supervisor and then adopted by the Commission. After the completion of the processing on behalf of the controller, the processor should, at the choice of the controller, return or delete the personal data, unless there is a requirement to store that personal data under Union or Member State law to which the processor is subject.</p>	<p>processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject. The controller and processor should be able to choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by the European Data Protection Supervisor and then adopted by the Commission. After the completion of the processing on behalf of the controller, the processor should, at the choice of the controller, return or delete the personal data, unless there is a requirement to store that personal data under Union or Member State law to which the processor is subject.</p>



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>(42)</p> <p>In order to demonstrate compliance with this Regulation, controllers should maintain records of processing activities under their responsibility and processors should maintain records of categories of processing activities under their responsibility. Union institutions and bodies should be obliged to cooperate with the European Data Protection Supervisor and make their records, on request, available to it, so that they might serve for monitoring those processing operations. Union institutions and bodies should be able to establish a central register of records of their processing activities. For reasons of transparency, they should also be able to make such a register public.</p>	<p><b>AM 16</b></p> <p>(42)</p> <p>In order to demonstrate compliance with this Regulation, controllers should maintain records of processing activities under their responsibility and processors should maintain records of categories of processing activities under their responsibility. Union institutions and bodies should be obliged to cooperate with the European Data Protection Supervisor and make their records, on request, available to it, so that they might serve for monitoring those processing operations. Union institutions and bodies should <del>be able to</del> establish a central register of records of their processing activities. For reasons of transparency, they should <del>also be able to</del> <b><i>make such a register public.</i></b></p>	<p>(42)</p> <p>In order to demonstrate compliance with this Regulation, controllers should maintain records of processing activities under their responsibility and processors should maintain records of categories of processing activities under their responsibility. Union institutions and bodies should be obliged to cooperate with the European Data Protection Supervisor and make their records, on request, available to it, so that they might serve for monitoring those processing operations. Union institutions and bodies should be able to establish a central register of records of their processing activities. For reasons of transparency, they should also be able to make such a register public.</p>	<p>Council suggestion:</p> <p>(42) In order to demonstrate compliance with this Regulation, controllers should maintain records of processing activities under their responsibility and processors should maintain records of categories of processing activities under their responsibility. Union institutions and bodies should be obliged to cooperate with the European Data Protection Supervisor and make their records, on request, available to it, so that they might serve for monitoring those processing operations. Unless it is not appropriate taking into account the size of the institution or agency, Union institutions and bodies should be able to establish a central register of records of their processing activities. For reasons of transparency, they should also be able to make such a register public.</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>(43)</p> <p>In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.</p>	<p>(43)</p> <p>In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.</p>	<p>(43)</p> <p>In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.</p>	

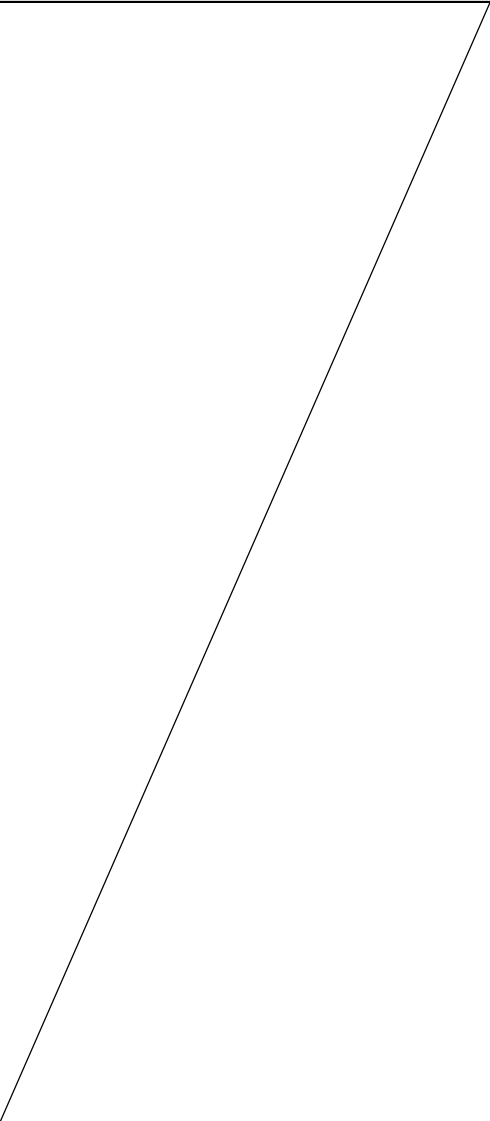
COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>(44)</p> <p>Union institutions and bodies should ensure the confidentiality of electronic communications as provided for by Article 7 of the Charter. In particular, Union institutions and bodies should ensure the security of their electronic communication networks, protect the information related to end-users' terminal equipment accessing their publicly available websites and mobile applications in accordance with Regulation (EU) XXXX/XX [new ePrivacy Regulation] and protect the personal data in directories of users.</p>	<p>(44)</p> <p>Union institutions and bodies should ensure the confidentiality of electronic communications as provided for by Article 7 of the Charter. In particular, Union institutions and bodies should ensure the security of their electronic communication networks, protect the information related to end-users' terminal equipment accessing their publicly available websites and mobile applications in accordance with Regulation (EU) XXXX/XX [new ePrivacy Regulation] and protect the personal data in directories of users.</p>	<p>(44)</p> <p>Union institutions and bodies should ensure the confidentiality of electronic communications <b>data</b> as provided for by Article 7 of the Charter. In particular, Union institutions and bodies should ensure the security of their electronic communications<u>s</u> networks, protect the information related to end-users' terminal equipment accessing their publicly available websites and mobile applications in accordance with Regulation (EU) XXXX/XX [new ePrivacy Regulation] and protect the personal data in directories of users.</p>	<p>(44) Union institutions and bodies should ensure the confidentiality of electronic communications is provided for by Article 7 of the Charter. In particular, Union institutions and bodies should ensure the security of their electronic communications<u>s</u> networks, protect the information related to users' terminal equipment accessing their publicly available websites and mobile applications in accordance with the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) and protect the personal data in directories of users.</p>
<p>(45)</p> <p>A personal data breach could, if not addressed in an appropriate and timely manner, result in physical,</p>	<p>(45)</p> <p>A personal data breach could, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to</p>	<p>(45)</p> <p>A personal data breach could, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
material or non-material damage to natural persons. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify that personal data breach to the European Data Protection Supervisor without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, it should be accompanied by the reasons for the delay and information can be provided in phases without further undue delay. Where such delay is justified, less sensitive or less specific information on the breach should be released as early as possible, rather than fully resolving the underlying incident before notifying.	natural persons. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify that personal data breach to the European Data Protection Supervisor without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, it should be accompanied by the reasons for the delay and information can be provided in phases without further undue delay. Where such delay is justified, less sensitive or less specific information on the breach should be released as early as possible, rather than fully resolving the underlying incident before notifying.	natural persons. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify that personal data breach to the European Data Protection Supervisor without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, it should be accompanied by the reasons for the delay and information can be provided in phases without further undue delay. Where such delay is justified, less sensitive or less specific information on the breach should be released as early as possible, rather than fully resolving the underlying incident before notifying.	
(46)	(46)	(46)	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the European	The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the European	The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the European	
Data Protection Supervisor, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities.	Data Protection Supervisor, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities.	Data Protection Supervisor, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities.	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>(47)</p> <p>Regulation (EC) No 45/2001 provides for a general obligation of the controller to notify the processing of personal data to the data protection officer, who would in turn keep a register of processing operations notified. While that obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Such indiscriminate general notification obligations should therefore be abolished, and replaced by effective procedures and mechanisms which focus instead on those types of processing operations which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes. Such types of processing operations could be those which in, particular, involve using new technologies, or are of a new kind and where no data protection impact assessment has been carried out before by the controller, or where they become</p>	<p><b>AM 17</b></p> <p>47)</p> <p>Regulation (EC) No 45/2001 provides for a general obligation of the controller to notify the processing of personal data to the data protection officer, who <del>would</del> in turn <del>keep</del> <b>keeps</b> a register of processing operations notified. <del>While that obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Such indiscriminate general notification obligations should therefore be abolished, and replaced by effective procedures and mechanisms which focus instead on those types of</del> <b>Besides this general obligation, effective procedures and mechanisms should be put in place to monitor</b> processing operations <del>which</del> <b>that</b> are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes. Such types of processing operations</p>	<p>(47)</p> <p>Regulation (EC) No 45/2001 provides for a general obligation of the controller to notify the processing of personal data to the data protection officer, who would in turn keep a register of processing operations notified. While that obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Such indiscriminate general notification obligations should therefore be abolished, and replaced by effective procedures and mechanisms which focus instead on those types of processing operations which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes. Such types of processing operations could be those which in, particular, involve using new technologies, or are of a new kind and where no data protection impact assessment has</p>	<p>Council suggestion:</p> <p>(47)</p> <p>Regulation (EC) No 45/2001 provides for a general obligation of the controller to notify the processing of personal data to the data protection officer. Unless it is not appropriate taking into account the size of the institution or agency, the data protection officer keeps a register of processing operations notified. Besides this general obligation, effective procedures and mechanisms should be put in place to monitor processing operations that are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes. Such procedures should also be in place, in particular, where types of processing operations involve using new technologies, or are of a new kind and where no data protection impact assessment has been carried out before by the</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
necessary in the light of the time that has elapsed since the initial processing. In such cases, a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation.	<del>could be those which in, particular,</del> <b><i>procedures should also be in place, in particular, where types of processing operations</i></b> involve using new technologies, or are of a new kind and where no data protection impact assessment has been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing. In such cases, a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation.	been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing. In such cases, a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation.	controller, or where they become necessary in the light of the time that has elapsed since the initial processing. In such cases, a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation.

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>(48)</p> <p>Where a data protection impact assessment indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the European Data Protection Supervisor should be consulted prior to the start of processing activities. Such high risk is likely to result from certain types of processing and the extent and frequency of processing, which could result also in a realisation of damage or interference with the rights and freedoms of the natural person. The European Data Protection Supervisor should respond to the request for consultation within a specified period. However, the absence of a reaction of the European Data Protection Supervisor within that</p>	<p>(48)</p> <p>Where a data protection impact assessment indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the European Data Protection Supervisor should be consulted prior to the start of processing activities. Such high risk is likely to result from certain types of processing and the extent and frequency of processing, which could result also in a realisation of damage or interference with the rights and freedoms of the natural person. The European Data Protection Supervisor should respond to the request for consultation within a specified period. However, the absence of a reaction of the European Data Protection Supervisor within that</p>	<p>(48)</p> <p>Where a data protection impact assessment indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the European Data Protection Supervisor should be consulted prior to the start of processing activities. Such high risk is likely to result from certain types of processing and the extent and frequency of processing, which could result also in a realisation of damage or interference with the rights and freedoms of the natural person. The European Data Protection Supervisor should respond to the request for consultation within a specified period. However, the absence of a reaction of the European Data</p>	



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
period should be without prejudice to any intervention of the European Data Protection Supervisor in accordance with its tasks and powers laid down in this Regulation, including the power to prohibit processing operations. As part of that consultation process, it should be possible to submit the outcome of a data protection impact assessment carried out with regard to the processing at issue to the European Data Protection Supervisor, in particular the measures envisaged to mitigate the risk to the rights and freedoms of natural persons.	period should be without prejudice to any intervention of the European Data Protection Supervisor in accordance with its tasks and powers laid down in this Regulation, including the power to prohibit processing operations. As part of that consultation process, it should be possible to submit the outcome of a data protection impact assessment carried out with regard to the processing at issue to the European Data Protection Supervisor, in particular the measures envisaged to mitigate the risk to the rights and freedoms of natural persons.	Protection Supervisor within that period should be without prejudice to any intervention of the European Data Protection Supervisor in accordance with its tasks and powers laid down in this Regulation, including the power to prohibit processing operations. As part of that consultation process, it should be possible to submit the outcome of a data protection impact assessment carried out with regard to the processing at issue to the European Data Protection Supervisor, in particular the measures envisaged to mitigate the risk to the rights and freedoms of natural persons.	
(49)  The European Data Protection Supervisor should be informed about administrative measures and internal rules of Union institutions and bodies which provide for the processing of personal data, lay down conditions for restrictions of data subject rights or provide appropriate safeguards for data	(49)  The European Data Protection Supervisor should be informed about administrative measures <del>and internal rules</del> of Union institutions and bodies which provide for the processing of personal data, lay down conditions for restrictions of data subject rights or provide appropriate safeguards for data	(49)  The European Data Protection Supervisor should be informed about administrative measures and <b>consulted on</b> internal rules <del>of</del> <b>adopted by</b> Union institutions and bodies <b>in matters relating to their operation</b> which provide for the processing of personal data, lay down conditions for restrictions of	Council suggestion:  (49)  The European Data Protection Supervisor should be informed about administrative measures and consulted on internal rules adopted by Union institutions and bodies in matters relating to their operation which provide for the

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
subject rights, in order to ensure compliance of the intended processing with this Regulation and in particular to mitigate the risk involved for the data subject.	subject rights, in order to ensure compliance of the intended processing with this Regulation and in particular to mitigate the risk involved for the data subject.	data subject rights or provide appropriate safeguards for data subject rights, in order to ensure compliance of the intended processing with this Regulation and in particular to mitigate the risk involved for the data subject.	processing of personal data, lay down conditions for restrictions of data subject rights or provide appropriate safeguards for data subject rights, in order to ensure compliance of the intended processing with this Regulation and in particular to mitigate the risk involved for the data subject.
<p>(50)</p> <p>Regulation (EU) 2016/679 established the European Data Protection Board as an independent body of the Union with legal personality. The Board should contribute to the consistent application of Regulation (EU) 2016/679 and Directive 2016/680 throughout the Union, including by advising the Commission. At the same time, the European Data Protection Supervisor should continue to exercise its supervisory and advisory functions in respect of all Union institutions and bodies, including on its own initiative or upon request. In order to ensure consistency of data protection rules</p>	<p><b>AM 18</b></p> <p>(50)</p> <p>Regulation (EU) 2016/679 established the European Data Protection Board as an independent body of the Union with legal personality. The Board should contribute to the consistent application of Regulation (EU) 2016/679 and Directive 2016/680 throughout the Union, including by advising the Commission. At the same time, the European Data Protection Supervisor should continue to exercise its supervisory and advisory functions in respect of all Union institutions and bodies, including on its own initiative or</p>	<p>(50)</p> <p>Regulation (EU) 2016/679 established the European Data Protection Board as an independent body of the Union with legal personality. The Board should contribute to the consistent application of Regulation (EU) 2016/679 and Directive 2016/680 throughout the Union, including by advising the Commission. At the same time, the European Data Protection Supervisor should continue to exercise its supervisory and advisory functions in respect of all Union institutions and bodies, including on its own initiative or upon request. In order to ensure consistency of data</p>	<p>Council suggestion:</p> <p>(50) Regulation (EU) 2016/679 established the European Data Protection Board as an independent body of the Union with legal personality. The Board should contribute to the consistent application of Regulation (EU) 2016/679 and Directive 2016/680 throughout the Union, including by advising the Commission. At the same time, the European Data Protection Supervisor should continue to exercise its supervisory and advisory functions in respect of all Union institutions and bodies, including on its own initiative or upon request. In order to ensure</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
throughout the Union, a consultation by the Commission should be obligatory following the adoption of legislative acts or during the preparation of delegated acts and implementing acts as defined in Article 289, 290 and 291 TFEU and following the adoption of recommendations and proposals relating to agreements with third countries and international organisations as provided for in Article 218 TFEU, which have an impact on the right to personal data protection. In such cases, the Commission should be obliged to consult the European Data Protection Supervisor, except when the Regulation (EU) 2016/679 provides for mandatory consultation of the European Data Protection Board, for example on adequacy decisions or delegated acts on standardised icons and requirements for certification mechanisms. Where the act in question is of particular importance for the protection of individuals' rights and freedoms with regard to the processing of personal data, the Commission	upon request. In order to ensure consistency of data protection rules throughout the Union, a consultation by the Commission should be obligatory <del>following the adoption of legislative acts</del> <b>when adopting proposals for a legislative act</b> or during the preparation of delegated acts and implementing acts as defined in Article 289, 290 and 291 TFEU and <del>following the adoption of</del> <b>when adopting</b> recommendations and proposals relating to agreements with third countries and international organisations as provided for in Article 218 TFEU, which have an impact on the right to personal data protection. In such cases, the Commission should be obliged to consult the European Data Protection Supervisor, except when the Regulation (EU) 2016/679 provides for mandatory consultation of the European Data Protection Board, for example on adequacy decisions or delegated acts on standardised icons and requirements for certification mechanisms. Where the act in question is of particular	protection rules throughout the Union, a consultation by the Commission should be obligatory following the adoption of legislative acts or during the preparation of delegated acts and implementing acts as defined in Article 289, 290 and 291 TFEU and following the adoption of recommendations and proposals relating to agreements with third countries and international organisations as provided for in Article 218 TFEU, which have an impact on the right to personal data protection. In such cases, the Commission should be obliged to consult the European Data Protection Supervisor, except when the Regulation (EU) 2016/679 provides for mandatory consultation of the European Data Protection Board, for example on adequacy decisions or delegated acts on standardised icons and requirements for certification mechanisms. Where the act in question is of particular importance for the protection of individuals' rights and freedoms with regard to	consistency of data protection rules throughout the Union, when preparing proposals or recommendations, the Commission should endeavour to consult the EDPS. A consultation by the Commission should be obligatory following the adoption of legislative acts or during the preparation of delegated acts and implementing acts as defined in Article 289, 290 and 291 TFEU and following the adoption of recommendations and proposals relating to agreements with third countries and international organisations as provided for in Article 218 TFEU, which have an impact on the right to personal data protection. In such cases, the Commission should be obliged to consult the European Data Protection Supervisor, except when the Regulation (EU) 2016/679 provides for mandatory consultation of the European Data Protection Board, for example on adequacy decisions or delegated acts on standardised icons and requirements for certification

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>should be able, in addition, to consult the European Data Protection Board. In those cases, the European Data Protection Supervisor should, as a member of the European Data Protection Board, coordinate its work with the latter with a view to issue a joint opinion. The European Data Protection Supervisor, and where applicable, the European Data Protection Board should provide its written advice within eight weeks. That time-frame should be shorter in case of urgency or otherwise appropriate, for example when the Commission is preparing delegated and implementing acts.</p>	<p>importance for the protection of individuals' rights and freedoms with regard to the processing of personal data, the Commission should be able, in addition, to consult the European Data Protection Board. In those cases, the European Data Protection Supervisor should, as a member of the European Data Protection Board, coordinate its work with the latter with a view to issue a joint opinion. The European Data Protection Supervisor, and where applicable, the European Data Protection Board should provide its written advice within eight weeks. That time-frame should be shorter in case of urgency or otherwise appropriate, for example when the Commission is preparing delegated and implementing acts.</p>	<p>the processing of personal data, the Commission should be able, in addition, to consult the European Data Protection Board. In those cases, the European Data Protection Supervisor should, as a member of the European Data Protection Board, coordinate its work with the latter with a view to issue a joint opinion. The European Data Protection Supervisor, and where applicable, the European Data Protection Board should provide its written advice within eight weeks. That time-frame should be shorter in case of urgency or otherwise appropriate, for example when the Commission is preparing delegated and implementing acts.</p>	<p>mechanisms. Where the act in question is of particular importance for the protection of individuals' rights and freedoms with regard to the processing of personal data, the Commission should be able, in addition, to consult the European Data Protection Board. In those cases, the European Data Protection Supervisor should, as a member of the European Data Protection Board, coordinate its work with the latter with a view to issue a joint opinion. The European Data Protection Supervisor, and where applicable, the European Data Protection Board should provide its written advice within eight weeks. That time-frame should be shorter in case of urgency or otherwise appropriate, for example when the Commission is preparing delegated and implementing acts.</p>

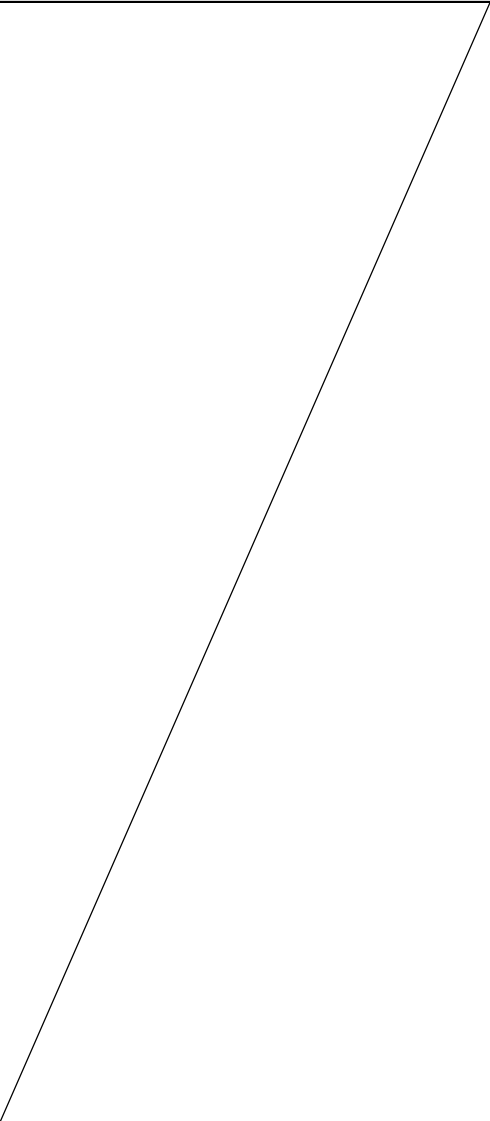
COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<p><b>AM 19</b></p> <p><b>(50a)</b></p> <p><i>I</i></p> <p><b><i>n accordance with Article 75 of Regulation (EU) 2016/679, the European Data Protection Supervisor will provide the secretariat of the European Data Protection Board.</i></b></p>		<p>(50a) In accordance with Article 75 of Regulation (EU) 2016/679, the European Data Protection Supervisor should provide the secretariat of the European Data Protection Board.</p>
<p>(51)</p> <p>In each Union institution or body a data protection officer should ensure that the provisions of this Regulation are applied and should advise controllers and processors on fulfilling their obligations. That officer should be a person with expert knowledge of data protection law and practices, which should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor. Such data protection officers should be in a position to perform their duties and tasks in an</p>	<p>(51)</p> <p>In each Union institution or body a data protection officer should ensure that the provisions of this Regulation are applied and should advise controllers and processors on fulfilling their obligations. That officer should be a person with expert knowledge of data protection law and practices, which should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor. Such data protection officers should be in a position to perform their duties and tasks in an</p>	<p>(51)</p> <p>In each Union institution or body a data protection officer should ensure that the provisions of this Regulation are applied and should advise controllers and processors on fulfilling their obligations. That officer should be a person with expert knowledge of data protection law and practices, which should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor. Such data protection officers should be in a position to perform their duties and tasks in an</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
independent manner.	independent manner.	independent manner.	
<p>(52)</p> <p>When personal data are transferred from the Union institutions and bodies to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are</p>	<p><b>AM 20</b></p> <p>(52)</p> <p>When personal data are transferred from the Union institutions and bodies to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should <del>not</del> be <del>undermined</del> <b>guaranteed</b>, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation, <b><i>with Regulation (EU) 2016/679 and with the fundamental rights and freedoms enshrined in the Charter.</i></b> A transfer could take place only if, subject to the other provisions of this Regulation, the</p>	<p>(52)</p> <p>When personal data are transferred from the Union institutions and bodies to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are</p>	<p>(52) When personal data are transferred from the Union institutions and bodies to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should be guaranteed, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation and with the fundamental rights and freedoms enshrined in the Charter. A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
complied with by the controller or processor.	conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor.	complied with by the controller or processor.	data to third countries or international organisations are complied with by the controller or processor.
<p>(53)</p> <p>The Commission can decide, under Article 45 of Regulation (EU) 2016/679, that a third country, a territory or specified sector within a third country, or an international organisation, offers an adequate level of data protection. In such cases, transfers of personal data to that third country or international organisation by a Union institution or body can take place without the need to obtain any further authorisation.</p>	<p><b>AM 21</b></p> <p>(53)</p> <p>The Commission can decide, under Article 45 of Regulation (EU) 2016/679 <i>or to Article 36 of Directive (EU) 2016/680</i>, that a third country, a territory or specified sector within a third country, or an international organisation, offers an adequate level of data protection. In such cases, transfers of personal data to that third country or international organisation by a Union institution or body can take place without the need to obtain any further authorisation.</p>	<p>(53)</p> <p>The Commission can decide, under Article 45 of Regulation (EU) 2016/679, that a third country, a territory or specified sector within a third country, or an international organisation, offers an adequate level of data protection. In such cases, transfers of personal data to that third country or international organisation by a Union institution or body can take place without the need to obtain any further authorisation.</p>	<p>(53)</p> <p>The Commission can decide, under Article 45 of Regulation (EU) 2016/679 or to Article 36 of Directive (EU) 2016/680, that a third country, a territory or specified sector within a third country, or an international organisation, offers an adequate level of data protection. In such cases, transfers of personal data to that third country or international organisation by a Union institution or body can take place without the need to obtain any further authorisation.</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>(54)</p> <p>In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards can consist of making use of standard data protection clauses adopted by the Commission, standard data protection clauses adopted by the European Data Protection Supervisor or contractual clauses authorised by the European Data Protection Supervisor. Where the processor is not a Union Institution or body those appropriate safeguards can also consist of binding corporate rules, codes of conduct and certification mechanisms used for international transfers under Regulation (EU) 2016/679. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects</p>	<p>(54)</p> <p>I</p> <p>n the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards can consist of making use of standard data protection clauses adopted by the Commission, standard data protection clauses adopted by the European Data Protection Supervisor or contractual clauses authorised by the European Data Protection Supervisor. Where the processor is not a Union Institution or body those appropriate safeguards can also consist of binding corporate rules, codes of conduct and certification mechanisms used for international transfers under Regulation (EU) 2016/679. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects</p>	<p>(54)</p> <p>In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards can consist of making use of standard data protection clauses adopted by the Commission, standard data protection clauses adopted by the European Data Protection Supervisor or contractual clauses authorised by the European Data Protection Supervisor. Where the processor is not a Union Institution or body those appropriate safeguards can also consist of binding corporate rules, codes of conduct and certification mechanisms used for international transfers under Regulation (EU) 2016/679. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects</p>	



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country. They should relate in particular to compliance with the general principles relating to personal data processing, the principles of data protection by design and by default. Transfers may also be carried out by Union institutions and bodies to public authorities or bodies in third countries or to international organisations with corresponding duties or functions, including on the basis of provisions to be inserted into administrative arrangements, such as a memorandum of understanding, providing for enforceable and effective rights for data subjects. Authorisation by the European Data Protection Supervisor should be obtained when the safeguards are provided for in administrative arrangements</p>	<p>appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country. They should relate in particular to compliance with the general principles relating to personal data processing, the principles of data protection by design and by default. Transfers may also be carried out by Union institutions and bodies to public authorities or bodies in third countries or to international organisations with corresponding duties or functions, including on the basis of provisions to be inserted into administrative arrangements, such as a memorandum of understanding, providing for enforceable and effective rights for data subjects. Authorisation by the European Data Protection Supervisor should be obtained when the safeguards are provided for in administrative arrangements that are</p>	<p>appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country. They should relate in particular to compliance with the general principles relating to personal data processing, the principles of data protection by design and by default. Transfers may also be carried out by Union institutions and bodies to public authorities or bodies in third countries or to international organisations with corresponding duties or functions, including on the basis of provisions to be inserted into administrative arrangements, such as a memorandum of understanding, providing for enforceable and effective rights for data subjects. Authorisation by the European Data Protection Supervisor should be obtained when the safeguards are provided for in administrative arrangements that are not legally</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
that are not legally binding.	not legally binding.	binding.	
<p>(55)</p> <p>The possibility for the controller or processor to use standard data-protection clauses adopted by the Commission or by the European Data Protection Supervisor should prevent controllers or processors neither from including the standard data-protection clauses in a wider contract, such as a contract between the processor and another processor, nor from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by the European Data Protection Supervisor or prejudice the</p>	<p>(55)</p> <p>The possibility for the controller or processor to use standard data-protection clauses adopted by the Commission or by the European Data Protection Supervisor should prevent controllers or processors neither from including the standard data-protection clauses in a wider contract, such as a contract between the processor and another processor, nor from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by the European Data Protection Supervisor or prejudice the</p>	<p>(55)</p> <p>The possibility for the controller or processor to use standard data-protection clauses adopted by the Commission or by the European Data Protection Supervisor should prevent controllers or processors neither from including the standard data-protection clauses in a wider contract, such as a contract between the processor and another processor, nor from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by the European Data Protection Supervisor or prejudice the</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
fundamental rights or freedoms of the data subjects. Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard data-protection clauses.	fundamental rights or freedoms of the data subjects. Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard data-protection clauses.	fundamental rights or freedoms of the data subjects. Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard data-protection clauses.	
<p>(56)</p> <p>Some third countries adopt laws, regulations and other legal acts which purport to directly regulate the processing activities of Union institutions and bodies. This may include judgments of courts or tribunals or decisions of administrative authorities in third countries requiring a controller or processor to transfer or disclose personal data, and which are not based on an international agreement in force between the requesting third country and the Union. The extraterritorial application of those laws, regulations and other legal acts may be in breach of international law and may impede</p>	<p>(56)</p> <p>Some third countries adopt laws, regulations and other legal acts which purport to directly regulate the processing activities of Union institutions and bodies. This may include judgments of courts or tribunals or decisions of administrative authorities in third countries requiring a controller or processor to transfer or disclose personal data, and which are not based on an international agreement in force between the requesting third country and the Union. The extraterritorial application of those laws, regulations and other legal acts may be in breach of international law and may impede</p>	<p>(56)</p> <p>Some third countries adopt laws, regulations and other legal acts which purport to directly regulate the processing activities of Union institutions and bodies. This may include judgments of courts or tribunals or decisions of administrative authorities in third countries requiring a controller or processor to transfer or disclose personal data, and which are not based on an international agreement in force between the requesting third country and the Union. The extraterritorial application of those laws, regulations and other legal acts may be in breach of international law and may impede</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>the attainment of the protection of natural persons ensured in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may be the case, inter alia, where disclosure is necessary for an important ground of public interest recognised in Union law.</p>	<p>the attainment of the protection of natural persons ensured in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may be the case, inter alia, where disclosure is necessary for an important ground of public interest recognised in Union law.</p>	<p>the attainment of the protection of natural persons ensured in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may be the case, inter alia, where disclosure is necessary for an important ground of public interest recognised in Union law.</p>	
<p>(57)</p> <p>Provision should be made in specific situations for the possibility for transfers in certain circumstances where the data subject has given his or her explicit consent, where the transfer is occasional and necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies. Provision should also be made for the possibility for transfers where important grounds of public interest</p>	<p>(57)</p> <p>Provision should be made in specific situations for the possibility for transfers in certain circumstances where the data subject has given his or her explicit consent, where the transfer is occasional and necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies. Provision should also be made for the possibility for transfers where important grounds of public interest</p>	<p>(57)</p> <p>Provision should be made in specific situations for the possibility for transfers in certain circumstances where the data subject has given his or her explicit consent, where the transfer is occasional and necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies. Provision should also be made for the possibility for transfers where important grounds of public</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
laid down by Union law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In the latter case, such a transfer should not involve the entirety of the personal data or entire categories of the data contained in the register, unless authorised by Union law, and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or, if they are to be the recipients, taking into full account the interests and fundamental rights of the data subject.	laid down by Union law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In the latter case, such a transfer should not involve the entirety of the personal data or entire categories of the data contained in the register, unless authorised by Union law, and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or, if they are to be the recipients, taking into full account the interests and fundamental rights of the data subject.	interest laid down by Union law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In the latter case, such a transfer should not involve the entirety of the personal data or entire categories of the data contained in the register, unless authorised by Union law, and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or, if they are to be the recipients, taking into full account the interests and fundamental rights of the data subject.	
(58)  Those derogations should in particular apply to data transfers required and necessary for important reasons of public interest, for example in cases of international data exchange between Union institutions and bodies and	(58)  Those derogations should in particular apply to data transfers required and necessary for important reasons of public interest, for example in cases of international data exchange between Union institutions and bodies and	(58)  Those derogations should in particular apply to data transfers required and necessary for important reasons of public interest, for example in cases of international data exchange between Union institutions and	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
competition authorities, tax or customs administrations, financial supervisory authorities and services competent for social security matters or for public health, for example in the case of contact tracing for contagious diseases or in order to reduce and/or eliminate doping in sport. A transfer of personal data should also be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's or another person's vital interests, including physical integrity or life, if the data subject is incapable of giving consent. In the absence of an adequacy decision, Union law may, for	competition authorities, tax or customs administrations, financial supervisory authorities and services competent for social security matters or for public health, for example in the case of contact tracing for contagious diseases or in order to reduce and/or eliminate doping in sport. A transfer of personal data should also be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's or another person's vital interests, including physical integrity or life, if the data subject is incapable of giving consent. In the absence of an adequacy decision, Union law may, for	bodies and competition authorities, tax or customs administrations, financial supervisory authorities and services competent for social security matters or for public health, for example in the case of contact tracing for contagious diseases or in order to reduce and/or eliminate doping in sport. A transfer of personal data should also be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's or another person's vital interests, including physical integrity or life, if the data subject is incapable of giving consent. In the absence of an adequacy decision, Union law may, for	
important reasons of public interest, expressly set limits to the transfer of specific categories of data to a third country or an international organisation. Any transfer to an international humanitarian organisation of personal data of a data subject who is physically or legally incapable of giving consent, with a view to accomplishing a task	important reasons of public interest, expressly set limits to the transfer of specific categories of data to a third country or an international organisation. Any transfer to an international humanitarian organisation of personal data of a data subject who is physically or legally incapable of giving consent, with a view to accomplishing a task	important reasons of public interest, expressly set limits to the transfer of specific categories of data to a third country or an international organisation. Any transfer to an international humanitarian organisation of personal data of a data subject who is physically or legally incapable of giving consent, with a view to	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
incumbent under the Geneva Conventions or to complying with international humanitarian law applicable in armed conflicts, could be considered to be necessary for an important reason of public interest or because it is in the vital interest of the data subject.	incumbent under the Geneva Conventions or to complying with international humanitarian law applicable in armed conflicts, could be considered to be necessary for an important reason of public interest or because it is in the vital interest of the data subject.	accomplishing a task incumbent under the Geneva Conventions or to complying with international humanitarian law applicable in armed conflicts, could be considered to be necessary for an important reason of public interest or because it is in the vital interest of the data subject.	
(59)  In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with enforceable and effective rights as regards the processing of their data in the Union once those data have been transferred so that that they will continue to benefit from fundamental rights and safeguards.	(59)  In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with enforceable and effective rights as regards the processing of their data in the Union once those data have been transferred so that that they will continue to benefit from fundamental rights and safeguards.	(59)  In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with enforceable and effective rights as regards the processing of their data in the Union once those data have been transferred so that they will continue to benefit from fundamental rights and safeguards.	
(60)  When personal data moves across borders outside the Union it may put at increased risk the ability of	(60)  When personal data moves across borders outside the Union it may put at increased risk the ability of	(60)  When personal data moves across borders outside the Union it may put at increased risk the ability of	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities in the Union, including the European Data Protection Supervisor, can be unable to pursue complaints or conduct investigations relating to the activities outside their jurisdiction. Their efforts to work together in the cross-border context can also be hampered by insufficient preventive or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, closer cooperation between the European Data Protection Supervisor and other data protection supervisory authorities should be promoted to help the exchange of information with their international counterparts.	natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities in the Union, including the European Data Protection Supervisor, can be unable to pursue complaints or conduct investigations relating to the activities outside their jurisdiction. Their efforts to work together in the cross-border context can also be hampered by insufficient preventive or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, closer cooperation between the European Data Protection Supervisor and other data protection supervisory authorities should be promoted to help the exchange of information with their international counterparts.	natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities in the Union, including the European Data Protection Supervisor, can be unable to pursue complaints or conduct investigations relating to the activities outside their jurisdiction. Their efforts to work together in the cross-border context can also be hampered by insufficient preventive or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, closer cooperation between the European Data Protection Supervisor and other data protection supervisory authorities should be promoted to help the exchange of information with their international counterparts.	
(61)  The establishment of the European Data Protection Supervisor in	(61)  The establishment of the European Data Protection Supervisor in	(61)  The establishment of the European Data Protection Supervisor in	(61) The establishment of the European Data Protection Supervisor in Regulation (EC) No 45/2001, empowered to perform



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
Regulation (EC) No 45/2001, empowered to perform its tasks and exercise its powers with complete independence, is an essential component of the protection of natural persons with regard to the processing of their personal data. This Regulation should further strengthen and clarify its role and independence.	Regulation (EC) No 45/2001, empowered to perform its tasks and exercise its powers with complete independence, is an essential component of the protection of natural persons with regard to the processing of their personal data. This Regulation should further strengthen and clarify its role and independence.	Regulation (EC) No 45/2001, empowered to perform its tasks and exercise its powers with complete independence, is an essential component of the protection of natural persons with regard to the processing of their personal data. This Regulation should further strengthen and clarify its role and independence. <b>The European Data Protection Supervisor should be a person whose independence is beyond doubt and who is acknowledged as having the experience and skills required to perform the duties of European Data Protection Supervisor, for example because he or she has belonged to one of the supervisory authorities established under Article 41 of Regulation (EU) 2016/679.</b>	its tasks and exercise its powers with complete independence, is an essential component of the protection of natural persons with regard to the processing of their personal data. This Regulation should further strengthen and clarify its role and independence. The European Data Protection Supervisor should be a person whose independence is beyond doubt and who is acknowledged as having the experience and skills required to perform the duties of European Data Protection Supervisor, for example because he or she has belonged to one of the supervisory authorities established under Article 51 of Regulation (EU) 2016/679.
(62)  In order to ensure consistent monitoring and enforcement of data protection rules throughout the Union, the European Data	(62)  In order to ensure consistent monitoring and enforcement of data protection rules throughout the Union, the European Data	(62)  In order to ensure consistent monitoring and enforcement of data protection rules throughout the Union, the European Data	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
Protection Supervisor should have the same tasks and effective powers as the supervisory authorities in Member States, including powers of investigation, corrective powers and sanctions, and authorisation and advisory powers, in particular in cases of complaints from natural persons, and to bring infringements of this Regulation to the attention of the Court of Justice of the European Union and engage in legal proceedings in accordance with the primary law. Such powers should also include the power to impose a temporary or definitive limitation, including a ban, on processing. In order to avoid superfluous costs and excessive inconveniencies for the persons concerned who might be adversely affected, each measure of the European Data Protection Supervisor should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, should take into account the circumstances of each individual case and respect the right of every person to be heard before taking any individual measure. Each legally	Protection Supervisor should have the same tasks and effective powers as the supervisory authorities in Member States, including powers of investigation, corrective powers and sanctions, and authorisation and advisory powers, in particular in cases of complaints from natural persons, and to bring infringements of this Regulation to the attention of the Court of Justice of the European Union and engage in legal proceedings in accordance with the primary law. Such powers should also include the power to impose a temporary or definitive limitation, including a ban, on processing. In order to avoid superfluous costs and excessive inconveniencies for the persons concerned who might be adversely affected, each measure of the European Data Protection Supervisor should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, should take into account the circumstances of each individual case and respect the right of every person to be heard before taking any individual measure. Each legally	Protection Supervisor should have the same tasks and effective powers as the supervisory authorities in Member States, including powers of investigation, corrective powers and sanctions, and authorisation and advisory powers, in particular in cases of complaints from natural persons, and to bring infringements of this Regulation to the attention of the Court of Justice of the European Union and engage in legal proceedings in accordance with the primary law. Such powers should also include the power to impose a temporary or definitive limitation, including a ban, on processing. In order to avoid superfluous costs and excessive inconveniencies for the persons concerned who might be adversely affected, each measure of the European Data Protection Supervisor should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, should take into account the circumstances of each individual case and respect the right of every	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
binding measure of the European Data Protection Supervisor should be in writing, be clear and unambiguous, indicate the date of issue of the measure, bear the signature of the European Data Protection Supervisor, give the reasons for the measure, and refer to the right of an effective remedy.	binding measure of the European Data Protection Supervisor should be in writing, be clear and unambiguous, indicate the date of issue of the measure, bear the signature of the European Data Protection Supervisor, give the reasons for the measure, and refer to the right of an effective remedy.	person to be heard before taking any individual measure. Each legally binding measure of the European Data Protection Supervisor should be in writing, be clear and unambiguous, indicate the date of issue of the measure, bear the signature of the European Data Protection Supervisor, give the reasons for the measure, and refer to the right of an effective remedy.	
		<p><b>(62a)</b></p> <p><b>The supervisory competence of the European Data Protection Supervisor should not cover the processing of personal data by the Court of Justice of the European Union when acting in its judicial capacity, in order to safeguard the independence of the Court in the performance of its judicial tasks, including decision-making. For such processing operations, the Court should establish independent supervision, in accordance with Article 8(3) of the Charter, for</b></p>	<p><b>(62a)</b> The supervisory competence of the European Data Protection Supervisor should not cover the processing of personal data by the Court of Justice of the European Union when acting in its judicial capacity, in order to safeguard the independence of the Court in the performance of its judicial tasks, including decision-making. For such processing operations, the Court should establish independent supervision, in accordance with Article 8(3) of the Charter, for example through an internal mechanism.</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
		<b>example through an internal mechanism.</b>	
<p>(63)</p> <p>The decisions of the European Data Protection Supervisor regarding exemptions, guarantees, authorisations and conditions relating to data processing operations, as defined in this Regulation, should be published in the activities report. Independently of the publication of an annual activities report, the European Data Protection Supervisor can publish reports on specific subjects.</p>	<p>(63)</p> <p>The decisions of the European Data Protection Supervisor regarding exemptions, guarantees, authorisations and conditions relating to data processing operations, as defined in this Regulation, should be published in the activities report. Independently of the publication of an annual activities report, the European Data Protection Supervisor can publish reports on specific subjects.</p>	<p>(63)</p> <p>The decisions of the European Data Protection Supervisor regarding exemptions, guarantees, authorisations and conditions relating to data processing operations, as defined in this Regulation, should be published in the activities report. Independently of the publication of an annual activities report, the European Data Protection Supervisor can publish reports on specific subjects.</p>	
		<p><b>(63a)The European Data Protection Supervisor should comply with Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.</b></p>	<p>(63a)The European Data Protection Supervisor should comply with Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.</p>
<p>(64)</p>	<p>(64)</p>	<p>(64)</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
The national supervisory authorities monitor the application of Regulation (EU) 2016/679 and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market. In order to increase the consistency in application of data protection rules applicable in Member States and data protection rules applicable to Union institutions and bodies, the European Data Protection Supervisor should effectively cooperate with the national supervisory authorities.	The national supervisory authorities monitor the application of Regulation (EU) 2016/679 and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market. In order to increase the consistency in application of data protection rules applicable in Member States and data protection rules applicable to Union institutions and bodies, the European Data Protection Supervisor should effectively cooperate with the national supervisory authorities.	The national supervisory authorities monitor the application of Regulation (EU) 2016/679 and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market. In order to increase the consistency in application of data protection rules applicable in Member States and data protection rules applicable to Union institutions and bodies, the European Data Protection Supervisor should effectively cooperate with the national supervisory authorities.	
	<p><b>AM 22</b></p> <p><b>(64a)</b></p> <p><i>The Commission has proposed to amend Regulation (EU) No 1024/2012 of the European Parliament and of the Council of 25 October 2012 on administrative cooperation through the Internal</i></p>		deletion

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<p><i>Market Information System and repealing Commission Decision 2008/49/EC ('the IMI Regulation') to allow the IMI System to be used not only by the competent authorities of the Member States and the Commission, but also by Union bodies, offices and agencies<sup>1a</sup>. Pending this revision, the European Data Protection Supervisor and the European Data Protection Board should be able to use the Internal Market Information System for the purposes of administrative cooperation and information exchange stipulated in the General Data Protection Regulation in view of its entry into application on 25 May 2018.</i></p> <hr/> <p><sup>1a</sup> See Article 36 of the Proposal for a Regulation of the European Parliament</p>		
<p>(65)</p> <p>In certain instances, Union law provides for a model of coordinated supervision, shared between the</p>	<p><b>AM 23</b></p> <p>(65)</p> <p>In certain instances, Union law</p>	<p>(65)</p> <p>In certain instances, Union law provides for a model of</p>	<p>(65)</p> <p>In certain instances, Union law provides for a model of coordinated supervision, shared</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
European Data Protection Supervisor and the national supervisory authorities. Moreover, the European Data Protection Supervisor is the supervisory authority of Europol and a specific model of cooperation with the national supervisory authorities is established through a cooperation board with an advisory function. In order to improve the effective supervision and enforcement of substantive data protection rules, a single, coherent model of coordinated supervision should be introduced in the Union. The Commission should therefore, where appropriate, submit legislative proposals with a view to amending Union legal acts providing for a model of coordinated supervision, in order to align them with the coordinated supervision model of this Regulation. The European Data Protection Board should serve as a single forum for ensuring the effective coordinated supervision across the board.	provides for a model of coordinated supervision, shared between the European Data Protection Supervisor and the national supervisory authorities. Moreover, the European Data Protection Supervisor is the supervisory authority of Europol and a specific model of cooperation with the national supervisory authorities is established through a cooperation board with an advisory function. In order to improve the effective supervision and enforcement of substantive data protection rules, <del>be introduced in the Union. The Commission should therefore, where appropriate, submit legislative proposals with a view to amending Union legal acts providing for</del> <b>this Regulation should introduce</b> a single, coherent model of coordinated supervision, <del>in order to align them with the coordinated supervision model of this Regulation.</del> The European Data Protection Board should serve as a single forum for ensuring the effective coordinated supervision across the board.	coordinated supervision, shared between the European Data Protection Supervisor and the national supervisory authorities. Moreover, the European Data Protection Supervisor is the supervisory authority of Europol and a specific model of cooperation with the national supervisory authorities is established through a cooperation board with an advisory function. In order to improve the effective supervision and enforcement of substantive data protection rules, a single, coherent model of coordinated supervision should be introduced in the Union. The Commission should therefore, where appropriate, submit legislative proposals with a view to amending Union legal acts providing for a model of coordinated supervision, in order to align them with the coordinated supervision model of this Regulation. The European Data Protection Board should serve as a single forum for ensuring the effective coordinated supervision	between the European Data Protection Supervisor and the national supervisory authorities. Moreover, the European Data Protection Supervisor is the supervisory authority of Europol and a specific model of cooperation with the national supervisory authorities is established through a cooperation board with an advisory function. In order to improve the effective supervision and enforcement of substantive data protection rules, a single, coherent model of coordinated supervision should be introduced in the Union. The Commission should therefore, where appropriate, submit legislative proposals with a view to amending Union legal acts providing for a model of coordinated supervision, in order to align them with the coordinated supervision model of this Regulation. The European Data Protection Board should serve as a single forum for ensuring the effective coordinated supervision across the board.

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
		across the board.	
<p>(66)</p> <p>Every data subject should have the right to lodge a complaint with the European Data Protection Supervisor, and the right to an effective judicial remedy before the Court of Justice of the European Union in accordance with the Treaties, if the data subject considers that his or her rights under this Regulation are infringed or where the European Data Protection Supervisor does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The European Data Protection Supervisor should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case</p>	<p>(66)</p> <p>Every data subject should have the right to lodge a complaint with the European Data Protection Supervisor, and the right to an effective judicial remedy before the Court of Justice of the European Union in accordance with the Treaties, if the data subject considers that his or her rights under this Regulation are infringed or where the European Data Protection Supervisor does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The European Data Protection Supervisor should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case</p>	<p>(66)</p> <p>Every data subject should have the right to lodge a complaint with the European Data Protection Supervisor, and the right to an effective judicial remedy before the Court of Justice of the European Union in accordance with the Treaties, if the data subject considers that his or her rights under this Regulation are infringed or where the European Data Protection Supervisor does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The European Data Protection Supervisor should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case</p>	



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
requires further coordination with a national supervisory authority, intermediate information should be given to the data subject. In order to facilitate the submission of complaints, the European Data Protection Supervisor should take measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.	requires further coordination with a national supervisory authority, intermediate information should be given to the data subject. In order to facilitate the submission of complaints, the European Data Protection Supervisor should take measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication	requires further coordination with a national supervisory authority, intermediate information should be given to the data subject. In order to facilitate the submission of complaints, the European Data Protection Supervisor should take measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.	
(67)  Any person who has suffered material or non-material damage as a result of an infringement of this Regulation should have the right to receive compensation from the controller or processor for the damage suffered, subject to the conditions provided for in the Treaty.	(67)  Any person who has suffered material or non-material damage as a result of an infringement of this Regulation should have the right to receive compensation from the controller or processor for the damage suffered, subject to the conditions provided for in the Treaty.	(67)  Any person who has suffered material or non-material damage as a result of an infringement of this Regulation should have the right to receive compensation from the controller or processor for the damage suffered, subject to the conditions provided for in the Treaty.	
(68)  In order to strengthen the supervisory role of the European Data Protection Supervisor and the	(68)  In order to strengthen the supervisory role of the European Data Protection Supervisor and the	(68)  In order to strengthen the supervisory role of the European Data Protection Supervisor and the	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
effective enforcement of this Regulation, the European Data Protection Supervisor should, as a sanction of last resort, have the power to impose administrative fines. The fines should aim at sanctioning the institution or body – rather than individuals – for non-compliance with this Regulation, to deter future violations of this Regulation and to foster a culture of personal data protection within the Union institutions and bodies.	effective enforcement of this Regulation, the European Data Protection Supervisor should, as a sanction of last resort, have the power to impose administrative fines. The fines should aim at sanctioning the institution or body – rather than individuals – for non-compliance with this Regulation, to deter future violations of this Regulation and to foster a culture of personal data protection within the Union institutions and bodies.	effective enforcement of this Regulation, the European Data Protection Supervisor should, as a sanction of last resort, have the power to impose administrative fines. The fines should aim at sanctioning the institution or body – rather than individuals – for non-compliance with this Regulation, to deter future violations of this Regulation and to foster a culture of personal data protection within the Union institutions and bodies.	
This Regulation should indicate infringements and the upper limits and criteria for setting the related administrative fines. The European Data Protection Supervisor should determine the amount of fines in each individual case, by taking into account all relevant circumstances of the specific situation, with due regard to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement.	This Regulation should indicate infringements and the upper limits and criteria for setting the related administrative fines. The European Data Protection Supervisor should determine the amount of fines in each individual case, by taking into account all relevant circumstances of the specific situation, with due regard to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement.	This Regulation should indicate infringements and the upper limits and criteria for setting the related administrative fines. The European Data Protection Supervisor should determine the amount of fines in each individual case, by taking into account all relevant circumstances of the specific situation, with due regard to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
When imposing an administrative fine on a Union body, the European Data Protection Supervisor should consider the proportionality of amount of the fine. The administrative procedure for the imposition of fines on Union institutions and bodies should respect the general principles of Union law as interpreted by the Court of Justice of the European Union.	When imposing an administrative fine on a Union body, the European Data Protection Supervisor should consider the proportionality of amount of the fine. The administrative procedure for the imposition of fines on Union institutions and bodies should respect the general principles of Union law as interpreted by the Court of Justice of the European Union.	infringement. When imposing an administrative fine on a Union body, the European Data Protection Supervisor should consider the proportionality of amount of the fine. The administrative procedure for the imposition of fines on Union institutions and bodies should respect the general principles of Union law as interpreted by the Court of Justice of the European Union.	
(69)  Where a data subject considers that his or her rights under this Regulation are infringed, he or she should have the right to mandate a not-for-profit body, organisation or association which is constituted in accordance with Union law or the law of a Member State, has statutory objectives which are in the public interest and is active in the field of the protection of personal data to lodge a complaint on his or her behalf with the European Data Protection Supervisor. Such a body,	(69)  Where a data subject considers that his or her rights under this Regulation are infringed, he or she should have the right to mandate a not-for-profit body, organisation or association which is constituted in accordance with Union law or the law of a Member State, has statutory objectives which are in the public interest and is active in the field of the protection of personal data to lodge a complaint on his or her behalf with the European Data Protection Supervisor. Such a body,	(69)  Where a data subject considers that his or her rights under this Regulation are infringed, he or she should have the right to mandate a not-for-profit body, organisation or association which is constituted in accordance with Union law or the law of a Member State, has statutory objectives which are in the public interest and is active in the field of the protection of personal data to lodge a complaint on his or her behalf with the European Data Protection	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
organisation or association should also be able to exercise the right to a judicial remedy on behalf of data subjects or exercise the right to receive compensation on behalf of data subjects.	organisation or association should also be able to exercise the right to a judicial remedy on behalf of data subjects or exercise the right to receive compensation on behalf of data subjects.	Supervisor. Such a body, organisation or association should also be able to exercise the right to a judicial remedy on behalf of data subjects or exercise the right to receive compensation on behalf of data subjects.	
(70)  An official or other servant of the Union who fails to comply with the obligations in this Regulation should be liable to disciplinary or any other action, in accordance with the rules and procedures laid down in the Staff Regulations of Officials of the European Union or in the Conditions of Employment of Other Servants of the European Union.	(70)  An official or other servant of the Union who fails to comply with the obligations in this Regulation should be liable to disciplinary or any other action, in accordance with the rules and procedures laid down in the Staff Regulations of Officials of the European Union or in the Conditions of Employment of Other Servants of the European Union.	(70)  An official or other servant of the Union who fails to comply with the obligations in this Regulation should be liable to disciplinary or any other action, in accordance with the rules and procedures laid down in the Staff Regulations of Officials of the European Union or in the Conditions of Employment of Other Servants of the European Union.	
(71)  In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers	(71)  In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers	(71)  In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and the Council <sup>7</sup> . The examination	should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and the Council <sup>7</sup> . The examination	should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and the Council <sup>7</sup> . The examination	
procedure should be used for the adoption of standard contractual clauses between controllers and processors and between processors, for the adoption of list of processing operations where prior consultation of the European Data Protection Supervisor is required by controllers processing for the performance of a task carried out in the public interest, and for the adoption of standard contractual clauses providing appropriate safeguards for international transfers.	procedure should be used for the adoption of standard contractual clauses between controllers and processors and between processors, for the adoption of list of processing operations where prior consultation of the European Data Protection Supervisor is required by controllers processing for the performance of a task carried out in the public interest, and for the adoption of standard contractual clauses providing appropriate safeguards for international transfers.	procedure should be used for the adoption of standard contractual clauses between controllers and processors and between processors, for the adoption of list of processing operations where prior consultation of the European Data Protection Supervisor is required by controllers processing for the performance of a task carried out in the public interest, and for the adoption of standard contractual clauses providing appropriate safeguards for international transfers.	
(72)  The confidential information which the Union and national statistical authorities collect for the production of official European and official	(72)  The confidential information which the Union and national statistical authorities collect for the production of official European and official	(72)  The confidential information which the Union and national statistical authorities collect for the production of official European	

<sup>7</sup> Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
national statistics should be protected. European statistics should be developed, produced and disseminated in accordance with the statistical principles as set out in Article 338(2) TFEU. Regulation (EC) No 223/2009 of the European Parliament and of the Council <sup>8</sup> provides further specifications on statistical confidentiality for European statistics.	national statistics should be protected. European statistics should be developed, produced and disseminated in accordance with the statistical principles as set out in Article 338(2) TFEU. Regulation (EC) No 223/2009 of the European Parliament and of the Council <sup>9</sup> provides further specifications on statistical confidentiality for European statistics.	and official national statistics should be protected. European statistics should be developed, produced and disseminated in accordance with the statistical principles as set out in Article 338(2) TFEU. Regulation (EC) No 223/2009 of the European Parliament and of the Council <sup>9</sup> provides further specifications on statistical confidentiality for European statistics.	
(73)  Regulation (EC) No 45/2001 and Decision No 1247/2002/EC should be repealed. The references to the repealed Regulation and the Decision should be construed as references to this Regulation.	(73)  Regulation (EC) No 45/2001 and Decision No 1247/2002/EC should be repealed. The references to the repealed Regulation and the Decision should be construed as references to this Regulation.	(73)  Regulation (EC) No 45/2001 and Decision No 1247/2002/EC should be repealed. The references to the repealed Regulation and the Decision should be construed as references to this Regulation.	
(74)	(74)	(74)	

<sup>8</sup> Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities ([OJ L 87, 31.3.2009, p. 164](#)).

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
In order to safeguard the full independence of the members of the independent supervisory authority, the terms of office of the current European Data Protection Supervisor and the current Assistant Supervisor should not be affected by this Regulation. The current Assistant Supervisor should remain in place until the end of his term of office, unless one of the conditions for the premature end of term of the European Data Protection Supervisor laid down in this Regulation is met. The relevant provisions of this Regulation should apply to the Assistant Supervisor until the end of his term of office.	In order to safeguard the full independence of the members of the independent supervisory authority, the terms of office of the current European Data Protection Supervisor and the current Assistant Supervisor should not be affected by this Regulation. The current Assistant Supervisor should remain in place until the end of his term of office, unless one of the conditions for the premature end of term of the European Data Protection Supervisor laid down in this Regulation is met. The relevant provisions of this Regulation should apply to the Assistant Supervisor until the end of his term of office.	In order to safeguard the full independence of the members of the independent supervisory authority, the terms of office of the current European Data Protection Supervisor and the current Assistant Supervisor should not be affected by this Regulation. The current Assistant Supervisor should remain in place until the end of his term of office, unless one of the conditions for the premature end of term of the European Data Protection Supervisor laid down in this Regulation is met. The relevant provisions of this Regulation should apply to the Assistant Supervisor until the end of his term of office.	
(75)  In accordance with the principle of proportionality, it is necessary and appropriate for the achievement of the basic objective of ensuring an equivalent level of protection of natural persons and the free flow of personal data throughout the Union to lay down rules on processing of	(75)  In accordance with the principle of proportionality, it is necessary and appropriate for the achievement of the basic objective of ensuring an equivalent level of protection of natural persons and the free flow of personal data throughout the Union to lay down rules on processing of	(75)  In accordance with the principle of proportionality, it is necessary and appropriate for the achievement of the basic objective of ensuring an equivalent level of protection of natural persons and the free flow of personal data throughout the Union to lay down rules on processing of	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
personal data in Union institutions and bodies. This Regulation does not go beyond what is necessary in order to achieve the objectives pursued in accordance with Article 5(4) of the Treaty on European Union.	personal data in Union institutions and bodies. This Regulation does not go beyond what is necessary in order to achieve the objectives pursued in accordance with Article 5(4) of the Treaty on European Union.	personal data in Union institutions and bodies. This Regulation does not go beyond what is necessary in order to achieve the objectives pursued in accordance with Article 5(4) of the Treaty on European Union.	
(76)  The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on XX/XX/XXXX.	(76)  The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on XX/XX/XXXX.	(76)  The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on XX/XX/XXXX.	



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
HAVE ADOPTED THIS REGULATION:	HAVE ADOPTED THIS REGULATION:	HAVE ADOPTED THIS REGULATION:	
<b>CHAPTER I</b> <b>GENERAL PROVISIONS</b>	<b>CHAPTER I</b> <b>GENERAL PROVISIONS</b>	<b>CHAPTER I</b> <b>GENERAL PROVISIONS</b>	
<i>Article 1</i>	<i>Article 1</i>	<i>Article 1</i>	
<i>Subject-matter and objectives</i>	<i>Subject-matter and objectives</i>	<i>Subject-matter and objectives</i>	
1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and rules relating to the free movement of personal data	1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and rules relating to the free movement of personal data	1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data by the Union institutions <b>and</b> , bodies, <b>offices and agencies</b> and rules relating to the free movement of	1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data by the Union institutions and, bodies, and rules relating to the free movement of
between themselves or to recipients established in the Union and	between themselves or to recipients established in the Union and subject	personal data between themselves or to <b>other</b> recipients established in	personal data between themselves or to other recipients established

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
subject to Regulation (EU) 2016/679 <sup>9</sup> or the provisions of national law adopted pursuant to Directive (EU) 2016/680 <sup>10</sup> .	to Regulation (EU) 2016/679 <sup>10</sup> or the provisions of national law adopted pursuant to Directive (EU) 2016/680 <sup>11</sup> .	the Union <del>and subject to Regulation (EU) 2016/679<sup>9</sup> or the provisions of national law adopted pursuant to Directive (EU) 2016/680<sup>11</sup>.</del>	in the Union.
2.  This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.	<b>AM 24</b>  2.  This Regulation protects fundamental rights and freedoms of natural persons <i>enshrined in the Charter</i> and in particular their right to the protection of personal data.	2.  This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.	2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
3.  The European Data Protection Supervisor ('EDPS') shall monitor the application of the provisions of this Regulation to all processing	3.  The European Data Protection Supervisor ('EDPS') shall monitor the application of the provisions of this Regulation to all processing	3.  The European Data Protection Supervisor ('EDPS') shall monitor the application of the provisions of this Regulation to all processing	

<sup>9</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88.

<sup>10</sup> Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131.

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
operations carried out by a Union institution or body.	operations carried out by a Union institution or body.	operations carried out by a Union institution or body.	
<i>Article 2</i>	<i>Article 2</i>	<i>Article 2</i>	
<i>Scope</i>	<i>Scope</i>	<i>Scope</i>	
<p>1.</p> <p>This Regulation applies to the processing of personal data by all Union institutions and bodies insofar as such processing is carried out in the exercise of activities which fall, wholly or partially within the scope of Union law.</p>	<p><b>AM 25</b></p> <p>1.</p> <p>This Regulation applies to the processing of personal data by all Union institutions and bodies <del>insofar as such processing is carried out in the exercise of activities which fall, wholly or partially within the scope of Union law.</del></p>	<p>1.</p> <p>This Regulation applies to the processing of personal data by all Union institutions and bodies <del>insofar as such processing is carried out in the exercise of activities which fall, wholly or partially within the scope of Union law.</del></p>	<p>1. This Regulation applies to the processing of personal data by all Union institutions and bodies.</p>
		<p><b>1a.</b></p> <p><b>This Regulation shall not apply to the processing of operational personal data by Union bodies, offices or agencies carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU where the acts establishing those bodies, offices</b></p>	<p>1a. Only Article 3 and Chapter VIIIa shall apply to the processing of operational personal data by Union bodies, offices or agencies when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU.</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
		<b>or agencies provide for comprehensive rules relating to the protection of natural persons with regard to the processing of their data.</b>	
			1ab. This Regulation shall not apply to the processing of operational personal data by Europol and the European Public Prosecutor's Office, until Regulation (EU) 2016/794 and Regulation (EU) 2017/1939 are adapted in accordance with Article 70b.
		<b>1aa.</b> <b>This Regulation shall not apply to the processing of personal data by missions referred to in Articles 42(1), and 43 and 44 of the TEU.</b>	1ac. This Regulation shall not apply to the processing of personal data by missions referred to in Articles 42(1), 43 and 44 of the TEU.
2.  This Regulation shall apply to the processing of personal data, wholly or partially by automated means, and to the processing otherwise than by automated means of personal	2.  This Regulation shall apply to the processing of personal data, wholly or partially by automated means, and to the processing otherwise than by automated means of personal	2.  This Regulation shall apply to the processing of personal data, wholly or partially by automated means, and to the processing otherwise than by automated means of	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
data which form part of a filing system or are intended to form part of a filing system.	data which form part of a filing system or are intended to form part of a filing system.	personal data which form part of a filing system or are intended to form part of a filing system.	
	<p><b>AM 26</b></p> <p><i>2a.</i></p> <p><i>This Regulation shall also apply to Union agencies carrying out activities which fall within the scope of Chapters 4 and 5 of Title V of Part Three TFEU, including where the founding acts of these Union agencies lay down a stand-alone data protection regime for the processing of operational personal data. Provisions relating to specific processing of operational personal data contained in the founding acts of these agencies may particularise and complement the application of this Regulation.</i></p>		deletion
<i>Article 3</i>	<i>Article 3</i>	<i>Article 3</i>	
<i>Definitions</i>	<i>Definitions</i>	<i>Definitions</i>	
1.	1.	1.	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
For the purposes of this Regulation, the following definitions shall apply:	For the purposes of this Regulation, the following definitions shall apply:	For the purposes of this Regulation, the following definitions shall apply:	
			<p>(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;</p> <p>(2) 'operational personal data' means all personal data processed by Union bodies, offices or agencies carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU to meet the objectives and tasks laid down in the legal acts establishing these</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			<p>bodies, offices or agencies;</p> <p>(3) ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;</p> <p>(4) ‘restriction of processing’ means the marking of stored personal data with the aim of limiting their processing in the future;</p> <p>(5) ‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			<p>concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;</p> <p>(6) 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;</p> <p>(7) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;</p> <p>(8) 'controller' means the Union</p>



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			<p>institution, body, office or agency or the Directorate- General or any other organisational entity which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by a specific Union act, the controller or the specific criteria for its nomination can be provided for by Union law;</p> <p>(9) 'controllers other than Union institutions and bodies' means controllers within the meaning of Article 4(7) of Regulation (EU) 2016/679 and controllers within the meaning of Article 3(8) of Directive (EU) 2016/ 680;</p> <p>(10) 'Union institutions and bodies' means the Union institutions, bodies, offices and agencies set up by, or on the basis of, the Treaty on European Union, the Treaty on the Functioning of the European Union or the Euroatom Treaty;</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			<p>(11) 'competent authority' means a public authority in a Member State competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;</p> <p>(12) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller</p> <p>(13) 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			<p>compliance with the applicable data protection rules according to the purposes of the processing;</p> <p>(14) ‘third party’ means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;</p> <p>(15) ‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;</p> <p>(16) ‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			<p>(17) ‘genetic data’ means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;</p> <p>(18) ‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;</p> <p>(19) ‘data concerning health’ means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			<p>(20) ‘information society service’ means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council (19);</p> <p>(21) “international organisation” means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;</p> <p>(22) ‘national supervisory authority’ means an independent public authority which is established by a Member State pursuant to Article 51 of Regulation (EU) 2016/679 of the European Parliament and of the Council or pursuant to Article 41 of Directive (EU) 2016/680;</p> <p>(23) ‘user’ means any natural person using a network or terminal equipment operated under the control of a Union</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			<p>institution or body;</p> <p>(24) 'directory' means a publicly available directory of users or an internal directory of users available within a Union institution or body or shared between Union institutions and bodies, whether in printed or electronic form.</p> <p>(25) 'electronic communications network' means a transmission system, whether or not based on a permanent infrastructure or centralised administration capacity, and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit - and packet - switched including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed.  (26) the definition of ‘terminal equipment’ in point (1) of Article 1 of Commission Directive 2008/63/EC
(a)  the definitions in Regulation (EU) 2016/679, with the exception of the definition of ‘controller’ in point (7) of Article 4 of that Regulation;	<b>AM 27</b>  (a) the definitions in Regulation (EU) 2016/679, with the exception of the definition of 'controller' in point (7), <i>'main establishment' in point (16), 'enterprise' in point (18), 'group of undertaking' in point (19)</i> of Article 4 of that Regulation; <i>the definition of ‘electronic communication’ in point (a) of Article 4(2) of Regulation (EU) XX/XXXX [ePrivacy Regulation];</i>	(a)  the definitions in Regulation (EU) 2016/679, with the exception of the definition of ‘controller’ in point (7) of Article 4 of that Regulation;	deletion
(b)  the definition of ‘electronic communication’ in point (a) of	(b)  the definition of ‘electronic communication’ in point (a) of	(b)  the definition of ‘electronic communications <b>data</b> ’ in point (a)	deletion

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
Article 4(2) of Regulation (EU) XX/XXXX [ePrivacy Regulation];	Article 4(2) of Regulation (EU) XX/XXXX [ePrivacy Regulation];	of Article 4(3) of Regulation (EU) XX/XXXX [ePrivacy Regulation];	
(c)  the definitions of ‘electronic communication network’ and ‘end-user’ in points (1) and (14) of Article 2 of Directive 00/0000/EU [Directive establishing the European Electronic Communications Code] respectively;	(c)  the definitions of ‘electronic communication network’ and ‘end-user’ in points (1) and (14) of Article 2 of Directive 00/0000/EU [Directive establishing the European Electronic Communications Code] respectively;	(c)  the definitions of ‘electronic communications network’ and ‘end-user’ in points (1) and (14) of Article 2 of Directive 00/0000/EU [Directive establishing the European Electronic Communications Code] respectively;	deletion
(d)  the definition of ‘terminal equipment’ in point (1) of Article 1 of Commission Directive 2008/63/EC <sup>11</sup> .	(d)  the definition of ‘terminal equipment’ in point (1) of Article 1 of Commission Directive 2008/63/EC <sup>12</sup> .	(d)  the definition of ‘terminal equipment’ in point (1) of Article 1 of Commission Directive 2008/63/EC <sup>11</sup> .	deletion
2.  In addition, for the purposes of this Regulation the following definitions shall apply:	2.  In addition, for the purposes of this Regulation the following definitions shall apply:	2.  In addition, for the purposes of this Regulation the following definitions shall apply:	deletion

<sup>11</sup> Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment (OJ L 162 21.06.2008 p. 20).



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
(a)  'Union institutions and bodies' means the Union institutions, bodies, offices and agencies set up by, or on the basis of, the Treaty on European Union, the Treaty on the Functioning of the European Union or the Euroatom Treaty;	(a)  Union institutions and bodies' means the Union institutions, bodies, offices and agencies set up by, or on the basis of, the Treaty on European Union, the Treaty on the Functioning of the European Union or the Euroatom Treaty;	(a)  'Union institutions and bodies' means the Union institutions, bodies, offices and agencies set up by, or on the basis of, the Treaty on European Union, the Treaty on the Functioning of the European Union or the Euroatom Treaty;	deletion
		(aa)  <b>'Operational personal data' means personal data processed by Union bodies, offices or agencies carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU to meet the objectives laid down in the acts establishing these bodies, offices or agencies;</b>	deletion
(b)  'controller' means the Union institution, body, office or agency or the Directorate- General or any other organisational entity which, alone or jointly with others,	(b)  'controller' means the Union institution, body, office or agency or the Directorate- General or any other organisational entity which, alone or jointly with others,	(b)  'Controller' means the Union institution, body, office or agency or the Directorate- General or any other organisational entity which, alone or jointly with others,	deletion

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by a specific Union act, the controller or the specific criteria for its nomination can be provided for by Union law.	determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by a specific Union act, the controller or the specific criteria for its nomination can be provided for by Union law.	determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by a specific Union act, the controller or the specific criteria for its nomination can be provided for by Union law;	
		<b>(ba)</b>  <b>'Controllers other than Union institutions and bodies' means controllers within the meaning of Article 4(7) of Regulation (EU) 2016/679 and controllers within the meaning of Article 3(8) of Directive (EU) 2016/ 680;</b>	deletion
(c)  ‘user’ means any natural person using a network or terminal equipment operated under the control of a Union institution or body;	(c)  ‘user’ means any natural person using a network or terminal equipment operated under the control of a Union institution or body;	(c)  ‘user’ means any natural person using a network or terminal equipment operated under the control of a Union institution or body;	deletion

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>(d)</p> <p>‘directory’ means a publicly available directory of users or an internal directory of users available within a Union institution or body or shared between Union institutions and bodies, whether in printed or electronic form.</p>	<p>(d)</p> <p>‘directory’ means a publicly available directory of users or an internal directory of users available within a Union institution or body or shared between Union institutions and bodies, whether in printed or electronic form.</p>	<p>(d)</p> <p>‘directory’ means a publicly available directory of users or an internal directory of users available within a Union institution or body or shared between Union institutions and bodies, whether in printed or electronic form.</p>	deletion
	<p><b>AM 28</b></p> <p><i>(da)</i></p> <p><i>'operational personal data' means personal data processed by the Union agencies established on the basis of Chapters 4 and 5 of Title V of Part Three TFEU and by the missions referred to in Article 42(1), 43 and 44 TEU, for the purposes of meeting the objectives laid down in acts establishing those agencies or missions.</i></p>		deletion

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<b>CHAPTER I</b> <b>GENERAL PRINCIPLES</b>	<b>CHAPTER I</b> <b>GENERAL PRINCIPLES</b>	<b>CHAPTER I</b> <b>GENERAL PRINCIPLES</b>	
<i>Article 4</i>	<i>Article 4</i>	<i>Article 4</i>	
<i>Principles relating to processing of personal data</i>	<i>Principles relating to processing of personal data</i>	<i>Principles relating to processing of personal data</i>	
1. Personal data must be:	<b>AM 29</b> 1. Personal data <del>must</del> <b>shall</b> be:	1. Personal data must be:	1. Personal data shall be:
(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');	(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');	(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');	
(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving	(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving	(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 13, not be considered to be incompatible with the initial purposes ('purpose limitation');	purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 13, not be considered to be incompatible with the initial purposes ('purpose limitation');	purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 13, not be considered to be incompatible with the initial purposes ('purpose limitation');	
(c)  adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');	(c)  adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');	(c)  adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');	
(d)  accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified without delay ('accuracy');	<b>AM 30</b> (d)  accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that <del>data</del> <b>which personal data that</b> are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further <b>are</b> processed, are erased or rectified without delay ('accuracy');	(d)  accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that <b>personal</b> data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified without delay ('accuracy');	(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
(e)	(e)	(e)	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 13 subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');	kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 13 subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');	kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 13 subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');	
(f)  processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or	(f)  processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or	(f)  processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
organisational measures ('integrity and confidentiality').	organisational measures ('integrity and confidentiality').	organisational measures ('integrity and confidentiality').	
2.  The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').	2.  The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').	2.  The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').	
<i>Article 5</i>	<i>Article 5</i>	<i>Article 5</i>	
<i>Lawfulness of processing</i>	<i>Lawfulness of processing</i>	<i>Lawfulness of processing</i>	
1.  Processing shall be lawful only if and to the extent that at least one of the following applies:	1.  Processing shall be lawful only if and to the extent that at least one of the following applies:	1.  Processing shall be lawful only if and to the extent that at least one of the following applies:	
(a)  processing is necessary for the performance of a task carried out in the public interest on the basis or in the exercise of official authority vested in the Union institution or body;	(a)  processing is necessary for the performance of a task carried out in the public interest on the basis or in the exercise of official authority vested in the Union institution or body;	(a)  processing is necessary for the performance of a task carried out in the public interest <del>on the basis</del> or in the exercise of official authority vested in the Union institution or body;	(a) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body;
(b)	(b)	(b)	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
processing is necessary for compliance with a legal obligation to which the controller is subject;	processing is necessary for compliance with a legal obligation to which the controller is subject;	processing is necessary for compliance with a legal obligation to which the controller is subject;	
(c)  processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;	(c)  processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;	(c)  processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;	
(d)  the data subject has given consent to the processing of his or her personal data for one or more specific purposes;	(d)  the data subject has given consent to the processing of his or her personal data for one or more specific purposes;	(d)  the data subject has given consent to the processing of his or her personal data for one or more specific purposes;	
(e)  processing is necessary in order to protect the vital interests of the data subject or of another natural person.	(e)  processing is necessary in order to protect the vital interests of the data subject or of another natural person.	(e)  processing is necessary in order to protect the vital interests of the data subject or of another natural person.	
2.  The tasks referred to in point (a) of	<b>AM 31</b>  2.	2.  The <b>basis for the processing tasks</b>	2. The basis for the processing referred to in points (a) and (b) of paragraph 1 shall be laid down in



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
paragraph 1 shall be laid down in Union law.	The tasks referred to in point (a) of paragraph 1 shall be laid down in Union law. <i>The basis for the processing referred to in point (b) of paragraph 1 shall be laid down in Union or Member State law to which the controller is subject.</i>	referred to in points (a) <b>and (b)</b> of paragraph 1 shall be laid down in Union law.	Union law.
<i>Article 6</i>	<i>Article 6</i>	<i>Article 6</i>	
<i>Processing for another compatible purpose</i>	<i>Processing for another compatible purpose</i>	<i>Processing for another compatible purpose</i>	
Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on Union law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 25(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:	Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on Union law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 25(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:	Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on Union law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 25(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;	(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;	(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;	
(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;	(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;	(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;	
(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 10, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 11;	(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 10, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 11;	(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 10, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 11;	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
(d) the possible consequences of the intended further processing for data subjects;	(d) the possible consequences of the intended further processing for data subjects;	(d) the possible consequences of the intended further processing for data subjects;	
(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.	(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.	(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.	
<i>Article 7</i>	<i>Article 7</i>	<i>Article 7</i>	
<i>Conditions for consent</i>	<i>Conditions for consent</i>	<i>Conditions for consent</i>	
1.  Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.	1.  Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.	1.  Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.	
2.  If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for	2.  If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for	2.  If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.	consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.	consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.	
3.  The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.	3.  The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.	3.  The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.	
4.  When assessing whether consent is freely given, utmost account shall be taken of whether, <i>inter alia</i> , the performance of a contract, including	4.  When assessing whether consent is freely given, utmost account shall be taken of whether, <i>inter alia</i> , the performance of a contract, including	4.  When assessing whether consent is freely given, utmost account shall be taken of whether, <i>inter alia</i> , the performance of a contract,	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.	the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.	including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.	
<i>Article 8</i>	<i>Article 8</i>	<i>Article 8</i>	
<b>Conditions applicable to children's consent in relation to information society services</b>	<b>AM 32</b> Conditions applicable to <del>children's</del> <b>a child's</b> consent in relation to information society services	<b>Conditions applicable to children's consent in relation to information society services</b>	Conditions applicable to a child's consent in relation to information society services
1.  Where point (d) of Article 5(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 13 years old. Where the child is below the age of 13 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.	1.  Where point (d) of Article 5(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 13 years old. Where the child is below the age of 13 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.	1.  Where point (d) of Article 5(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 13 years old. Where the child is below the age of 13 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
2.  The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.	2.  The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.	2.  The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.	
3.	3.  Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.	3.  Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.	
	<b>AM 33</b>  <i>Article 8a</i>		
	<i>Transfer of personal data between Union institutions and bodies</i>		Council suggestion: deletion
	<i>Without prejudice to Articles 4, 5, 6 and 10:</i>		
	<i>1.</i>		

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<p><i>Personal data shall only be transferred within or to other Union institutions or bodies if the data are necessary for the legitimate performance of tasks covered by the competence of the recipient.</i></p>		
	<p>2.</p> <p><i>Where the data are transferred following a request from the recipient, both the controller and the recipient shall bear the responsibility for the legitimacy of this transfer.</i></p> <p><i>The controller shall be required to verify the competence of the recipient and to make a provisional evaluation of the necessity for the transfer of the data. If doubts arise as to this necessity, the controller shall seek further information from the recipient.</i></p> <p><i>The recipient shall ensure that the necessity for the transfer of the data can be subsequently verified.</i></p>		

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>3. The recipient shall process the personal data only for the purposes for which they were transmitted</i>		



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<i>Article 9</i>	<i>Article 9</i>	<i>Article 9</i>	<i>Article 9</i>
<i>Transmissions of personal data to recipients, other than Union institutions and bodies, established in the Union and subject to Regulation (EU) 2016/679 or Directive (EU) 2016/680</i>	<i>Transmissions of personal data to recipients, other than Union institutions and bodies, established in the Union and subject to Regulation (EU) 2016/679 or Directive (EU) 2016/680</i>	<i>Transmissions of personal data to recipients, other than Union institutions and bodies, established in the Union <del>and subject to Regulation (EU) 2016/679 or Directive (EU) 2016/680</del></i>	<i>Transmissions of personal data to recipients, other than Union institutions and bodies, established in the Union</i>
1.  Without prejudice to Articles 4, 5, 6 and 10, personal data shall only be transmitted to recipients established in the Union and subject to Regulation (EU) 2016/679 or to the national law adopted pursuant to Directive (EU) 2016/680, if the recipient establishes:	<b>AM 34</b>  1.  Without prejudice to Articles 4, 5, 6 <del>and 10, 10, 14, 15(3) and 16(4)</del> , personal data shall only be transmitted to recipients established in the Union and subject to Regulation (EU) 2016/679 or to the national law adopted pursuant to Directive (EU) 2016/680, if the <del>recipient</del> <b>controller</b> establishes, <b>on the basis of a reasoned request by the recipient</b> :	1.  Without prejudice to Articles 4, 5, 6 and 10, personal data shall only be transmitted to recipients, <b>other than Union institutions and bodies</b> , established in the Union <b>and subject to Regulation (EU) 2016/679 or to the national law adopted pursuant to Directive (EU) 2016/680</b> , if the recipient establishes:	Council suggestion: 1.  Without prejudice to Articles 4, 5, 6 and 10, personal data shall only be transmitted to recipients, other than Union institutions and bodies, established in the Union, if:
(a)  that the data are necessary for the performance of a task carried out in the public interest or subject to the	(a)  that the data are necessary for the performance of a task carried out in the public interest or subject to the	(a)  that the data are necessary for the performance of a task carried out in the public interest or <b>in subject</b>	(a) the recipient establishes that the data are necessary for the performance of a task carried out in the public interest or in the exercise of

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
exercise of official authority, or	<del>exercise of official authority, or</del>	<del>to</del> the exercise of official authority <b>vested in the recipient, or</b>	official authority vested in the recipient, or
(b)  that it is necessary to have the data transmitted, it is proportionate to the purposes of the transmission and if there is no reason to assume that the data subject's rights and freedoms and legitimate interests might be prejudiced.	<b>AM 35</b>  (b) <del>that it is to have the data transmitted, it is proportionate to the purposes of the transmission</del> <b>proportionate and necessary for the purpose of serving a public interest such as transparency or good administration</b> and, if there is <i>any</i> reason to assume that the data subject's rights and freedoms and legitimate interests might be prejudiced-, <b>after having demonstrably weighed the various competing interests;</b>	(b)  that it is necessary to have the data transmitted, it is proportionate to the purposes of the transmission and if there is no reason to assume that the data subject's rights and freedoms and legitimate interests might be prejudiced.	(b)  the recipient establishes that it is necessary to have the data transmitted for a specific purpose in the public interest and the controller, where there is any reason to assume that the data subject's legitimate interests might be prejudiced, establishes that it is proportionate to transmit the personal data for that specific purpose, after having demonstrably weighed the various competing interests.
2.  Where the transmission under this Article takes place on the initiative of the controller, the controller shall demonstrate that the transmission of personal data is necessary and proportionate to the purposes of the transmission, by applying the	2.  Where the transmission under this Article takes place on the initiative of the controller, the controller shall demonstrate that the transmission of personal data is necessary and proportionate to the purposes of the transmission, by applying the	2.  Where the transmission under this Article takes place on the initiative of the controller, the controller shall demonstrate that the transmission of personal data is necessary and proportionate to the purposes of the transmission, by	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
criteria laid down in points (a) or (b) of paragraph 1.	criteria laid down in points (a) or (b) of paragraph 1.	applying the criteria laid down in points (a) or (b) of paragraph 1.	
			(previous Article 70a) 3. Union institutions and bodies shall reconcile the right to the protection of personal data with the right of access to documents in accordance with Union law.
<i>Article 10</i>	<i>Article 10</i>	<i>Article 10</i>	
<i>Processing of special categories of personal data</i>	<i>Processing of special categories of personal data</i>	<i>Processing of special categories of personal data</i>	
1.  Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.	1.  Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.	1.  Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
2.  Paragraph 1 shall not apply if one of the following applies:	2.  Paragraph 1 shall not apply if one of the following applies:	2.  Paragraph 1 shall not apply if one of the following applies:	
(a)  the data subject has given explicit consent to the processing of those data for one or more specified purposes, except where Union law provides that the prohibition referred to in paragraph 1 may not be lifted by the data subject, or	<b>AM 36</b> (a) the data subject has given explicit consent to the processing of those <i>personal</i> data for one or more specified purposes, except where Union law provides that the prohibition referred to in paragraph 1 may not be lifted by the data subject, or	(a)  the data subject has given explicit consent to the processing of those data for one or more specified purposes, except where Union law provides that the prohibition referred to in paragraph 1 may not be lifted by the data subject, or	(a)  the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union law provides that the prohibition referred to in paragraph 1 may not be lifted by the data subject, or
(b)  processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law insofar as it is authorised by Union law providing for appropriate safeguards for the fundamental rights and the interests of the data subject, or	(b)  processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law insofar as it is authorised by Union law providing for appropriate safeguards for the fundamental rights and the interests	(b)  processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law insofar as it is authorised by Union law providing for appropriate safeguards for the fundamental rights and the interests of the data	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	of the data subject, or	subject, or	
(c)  processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent,	(c)  processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent,	(c)  processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent,	
(d)  processing is carried out in the course of its legitimate activities with appropriate safeguards by a non-profit-seeking body which constitutes an entity integrated in a Union institution or body and with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of this body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed outside that body without the consent of the data subjects;	(d)  processing is carried out in the course of its legitimate activities with appropriate safeguards by a non-profit-seeking body which constitutes an entity integrated in a Union institution or body and with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of this body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed outside that body without the consent of the data subjects;	(d)  processing is carried out in the course of its legitimate activities with appropriate safeguards by a non-profit-seeking body which constitutes an entity integrated in a Union institution or body and with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of this body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed outside that body without the consent of the data subjects;	
(e)	(e)	(e)	(e) processing relates to personal

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
processing relates to data which are manifestly made public by the data subject;	processing relates to data which are manifestly made public by the data subject;	processing relates to <b>personal</b> data which are manifestly made public by the data subject;	data which are manifestly made public by the data subject;
(f)  processing is necessary for the establishment, exercise or defence of legal claims or whenever the Court of Justice of the European Union is acting in its judicial capacity, or	(f)  processing is necessary for the establishment, exercise or defence of legal claims or whenever the Court of Justice of the European Union is acting in its judicial capacity, or	(f)  processing is necessary for the establishment, exercise or defence of legal claims or whenever the Court of Justice of the European Union is acting in its judicial capacity, or	
(g)  processing is necessary for reasons of substantial public interest, on the basis of Union law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;	(g)  processing is necessary for reasons of substantial public interest, on the basis of Union law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;	(g)  processing is necessary for reasons of substantial public interest, on the basis of Union law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;	
(h)  processing is necessary for the	(h)  processing is necessary for the	(h)  processing is necessary for the	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;	purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;	purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;	
(i)  processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;	(i)  processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;	(i)  processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>(j)</p> <p>processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes based on Union law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.</p>	<p>(j)</p> <p>processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes based on Union law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.</p>	<p>(j)</p> <p>processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes based on Union law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.</p>	
<p>3.</p> <p>Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union law.</p>	<p><b>AM 37</b></p> <p>3.</p> <p>Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union <del>law</del> <b><i>or Member State law or rules established by national competent bodies, or by another person also</i></b></p>	<p>3.</p> <p>Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union law.</p>	<p>3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies, or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national</p>



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.</i>		competent bodies.

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<i>Article 11</i>	<i>Article 11</i>	<i>Article 11</i>	
<i>Processing of personal data relating to criminal convictions and offences</i>	<i>Processing of personal data relating to criminal convictions and offences</i>	<i>Processing of personal data relating to criminal convictions and offences</i>	
Processing of personal data relating to criminal convictions and offences or related security measures pursuant to Article 5(1) may be carried out only if authorised by Union law, which may include internal rules, providing the appropriate specific safeguards for the rights and freedoms of data subjects.	<b>AM 38</b> Processing of personal data relating to criminal convictions and offences or related security measures pursuant to Article 5(1) <del>may</del> <b>shall</b> be carried out only if authorised by Union law, <del>which may include internal rules,</del> providing the appropriate specific safeguards for the rights and freedoms of data subjects.	Processing of personal data relating to criminal convictions and offences or related security measures pursuant to Article 5(1) <del>shall may</del> be carried out only <b>under control of official authority or when the processing is if</b> authorised by Union law; <del>which may include internal rules,</del> providing <del>for the</del> appropriate <del>specific</del> safeguards for the rights and freedoms of data subjects.	Processing of personal data relating to criminal convictions and offences or related security measures pursuant to Article 5(1) shall be carried out only under control of official authority or when the processing is authorised by Union law providing for appropriate safeguards for the rights and freedoms of data subjects.

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<i>Article 12</i>	<i>Article 12</i>	<i>Article 12</i>	
<b><i>Processing which does not require identification</i></b>	<b><i>Processing which does not require identification</i></b>	<b><i>Processing which does not require identification</i></b>	
<p>1.</p> <p>If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.</p>	<p>1.</p> <p>If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.</p>	<p>1.</p> <p>If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.</p>	
<p>2.</p> <p>Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 17 to 22 shall not apply except where the data subject, for the purpose of exercising his or her</p>	<p>2.</p> <p>Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 17 to 22 shall not apply except where the data subject, for the purpose of exercising his or her</p>	<p>2.</p> <p>Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 17 to 22 shall not apply except where the data subject, for the purpose of</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
rights under those articles, provides additional information enabling his or her identification.	rights under those articles, provides additional information enabling his or her identification.	exercising his or her rights under those articles, provides additional information enabling his or her identification.	
<i>Article 13</i>	<i>Article 13</i>	<i>Article 13</i>	
<i>Safeguards relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes</i>	<i>Safeguards relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes</i>	<i>Safeguards relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes</i>	
Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by	Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further	Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.	processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.	further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.	
<b>CHAPTER III</b>	<b>CHAPTER III</b>	<b>CHAPTER III</b>	
<b>RIGHTS OF THE DATA SUBJECT</b>	<b>RIGHTS OF THE DATA SUBJECT</b>	<b>RIGHTS OF THE DATA SUBJECT</b>	
<b>SECTION 1</b>	<b>SECTION 1</b>	<b>SECTION 1</b>	
<b>TRANSPARENCY AND MODALITIES</b>	<b>TRANSPARENCY AND MODALITIES</b>	<b>TRANSPARENCY AND MODALITIES</b>	
<i>Article 14</i>	<i>Article 14</i>	<i>Article 14</i>	
<i>Transparent information, communication and modalities for the exercise of the rights of the data subject</i>	<i>Transparent information, communication and modalities for the exercise of the rights of the data subject</i>	<i>Transparent information, communication and modalities for the exercise of the rights of the data subject</i>	
1.  The controller shall take appropriate measures to provide any information referred to in Articles 15 and 16 and any	1.  The controller shall take appropriate measures to provide any information referred to in Articles 15 and 16 and any	1.  The controller shall take appropriate measures to provide any information referred to in Articles 15 and 16 and any	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
communication under Articles 17 to 24 and 38 relating to processing to the data subject in a concise, transparent, intelligible and easily	communication under Articles 17 to 24 and 38 relating to processing to the data subject in a concise, transparent, intelligible and easily	communication under Articles 17 to 24 and 38 relating to processing to the data subject in a concise, transparent, intelligible and easily	
accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.	accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.	accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.	
2.  The controller shall facilitate the exercise of data subject rights under Articles 17 to 24. In the cases referred to in Article 12(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 17 to 24, unless the controller demonstrates that it is not in a position to identify the data	2.  The controller shall facilitate the exercise of data subject rights under Articles 17 to 24. In the cases referred to in Article 12(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 17 to 24, unless the controller demonstrates that it is not in a position to identify the data	2.  The controller shall facilitate the exercise of data subject rights under Articles 17 to 24. In the cases referred to in Article 12(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 17 to 24, unless the controller demonstrates that it is not in a position to identify the data	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
subject.	subject.	subject.	
<p>3.</p> <p>The controller shall provide information on action taken on a request under Articles 17 to 24 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.</p>	<p>3.</p> <p>The controller shall provide information on action taken on a request under Articles 17 to 24 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.</p>	<p>3.</p> <p>The controller shall provide information on action taken on a request under Articles 17 to 24 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.</p>	
<p>4.</p> <p>If the controller does not take action on the request of the data subject,</p>	<p>4.</p> <p>If the controller does not take action on the request of the data subject,</p>	<p>4.</p> <p>If the controller does not take action on the request of the data</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with the European Data Protection Supervisor and seeking a judicial remedy.	the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with the European Data Protection Supervisor and seeking a judicial remedy.	subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with the European Data Protection Supervisor and seeking a judicial remedy.	
5.  Information provided under Articles 15 and 16 and any communication and any actions taken under Articles 17 to 24 and 38 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may refuse to act on the request.	<b>AM 39</b>  Information provided under Articles 15 and 16 and any communication and any actions taken under Articles 17 to 24 and 38 shall be provided free of charge. <del>Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may refuse to act on the request.</del>	5.  Information provided under Articles 15 and 16 and any communication and any actions taken under Articles 17 to 24 and 38 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may refuse to act on the request.	5. Information provided under Articles 15 and 16 and any communication and any actions taken under Articles 17 to 24 and 38 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may refuse to act on the request.
The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.	The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.	The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.	The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.
6.	6.	6.	



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
Without prejudice to Article 12, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 17 to 23, the controller may request the provision of additional information necessary to confirm the identity of the data subject.	Without prejudice to Article 12, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 17 to 23, the controller may request the provision of additional information necessary to confirm the identity of the data subject.	Without prejudice to Article 12, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 17 to 23, the controller may request the provision of additional information necessary to confirm the identity of the data subject.	
7.  The information to be provided to data subjects pursuant to Articles 15 and 16 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.	7.  The information to be provided to data subjects pursuant to Articles 15 and 16 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.	7.  The information to be provided to data subjects pursuant to Articles 15 and 16 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.	
8.  If the Commission adopts delegated acts pursuant to Article 12(8) of Regulation (EU) 2016/679	<b>AM 40</b> 8. If The Commission <del>adopts</del> <b>shall be empowered to adopt</b> delegated acts pursuant to Article 12(8) of	8.  If the Commission adopts delegated acts pursuant to Article 12(8) of Regulation (EU)	8. If the Commission adopts delegated acts pursuant to Article 12(8) of Regulation (EU) 2016/679 determining the information to be presented by the

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
determining the information to be presented by the icons and the procedures for providing standardised icons, Union institutions and bodies shall, where appropriate, provide the information pursuant to Articles 15 and 16 in combination with such standardised icons.	Regulation (EU) 2016/679 determining the information to be presented by the icons and the procedures for providing standardised icons, Union institutions and bodies shall, where appropriate, provide the information pursuant to Articles 15 and 16 in combination with such standardised icons.	2016/679 determining the information to be presented by the icons and the procedures for providing standardised icons, Union institutions and bodies shall, where appropriate, provide the information pursuant to Articles 15 and 16 in combination with such standardised icons.	icons and the procedures for providing standardised icons, Union institutions and bodies shall, where appropriate, provide the information pursuant to Articles 15 and 16 in combination with such standardised icons.
<b>SECTION 2</b> <b>INFORMATION AND ACCESS TO PERSONAL DATA</b>	<b>SECTION 2</b> <b>INFORMATION AND ACCESS TO PERSONAL DATA</b>	<b>SECTION 2</b> <b>INFORMATION AND ACCESS TO PERSONAL DATA</b>	
<i>Article 15</i>	<i>Article 15</i>	<i>Article 15</i>	
<i>Information to be provided where personal data are collected from the data subject</i>	<i>Information to be provided where personal data are collected from the data subject</i>	<i>Information to be provided where personal data are collected from the data subject</i>	
1.  Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are	1.  Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are	1.  Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
obtained, provide the data subject with all of the following information:	obtained, provide the data subject with all of the following information:	obtained, provide the data subject with all of the following information:	
(a)  the identity and the contact details of the controller;	(a)  the identity and the contact details of the controller;	(a)  the identity and the contact details of the controller;	
(b)  the contact details of the data protection officer;	(b)  the contact details of the data protection officer;	(b)  the contact details of the data protection officer;	
(c)  the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;	(c)  the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;	(c)  the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;	
(d)  the recipients or categories of recipients of the personal data, if any;	(d)  the recipients or categories of recipients of the personal data, if any;	(d)  the recipients or categories of recipients of the personal data, if any;	
(e)  where applicable, the fact that the controller intends to transfer	(e)  where applicable, the fact that the	(e)  where applicable, the fact that the	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 49, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.	controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 49, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.	controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 49, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.	
2.  In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:	2.  In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:	2.  In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:	
(a)  the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;	(a)  the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;	(a)  the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>(b)</p> <p>the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or, where applicable, the right to object to processing or the right to data portability;</p>	<p>(b)</p> <p>the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or, where applicable, the right to object to processing or the right to data portability;</p>	<p>(b)</p> <p>the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or, where applicable, the right to object to processing or the right to data portability;</p>	
<p>(c)</p> <p>where the processing is based on point (d) of Article 5(1) or point (a) of Article 10(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;</p>	<p>(c)</p> <p>where the processing is based on point (d) of Article 5(1) or point (a) of Article 10(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;</p>	<p>(c)</p> <p>where the processing is based on point (d) of Article 5(1) or point (a) of Article 10(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;</p>	
<p>(d)</p> <p>the right to lodge a complaint with the European Data Protection Supervisor;</p>	<p>(d)</p> <p>the right to lodge a complaint with the European Data Protection Supervisor;</p>	<p>(d)</p> <p>the right to lodge a complaint with the European Data Protection Supervisor;</p>	
<p>(e)</p> <p>whether the provision of personal</p>	<p>(e)</p> <p>whether the provision of personal</p>	<p>(e)</p> <p>whether the provision of personal</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;	data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;	data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;	
(f)  the existence of automated decision-making, including profiling, referred to in Article 24(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;	(f)  the existence of automated decision-making, including profiling, referred to in Article 24(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;	(f)  the existence of automated decision-making, including profiling, referred to in Article 24(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;	
3.  Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that	3.  Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that	3.  Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
other purpose and with any relevant further information as referred to in paragraph 2.	other purpose and with any relevant further information as referred to in paragraph 2.	information on that other purpose and with any relevant further information as referred to in paragraph 2.	
4.  Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.	4.  Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.	4.  Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<i>Article 16</i>	<i>Article 16</i>	<i>Article 16</i>	
<i>Information to be provided where personal data have not been obtained from the data subject</i>	<i>Information to be provided where personal data have not been obtained from the data subject</i>	<i>Information to be provided where personal data have not been obtained from the data subject</i>	
1.  Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:	1.  Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:	1.  Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:	
(a)  the identity and the contact details of the controller;	(a)  the identity and the contact details of the controller;	(a)  the identity and the contact details of the controller;	
(b)  the contact details of the data protection officer;	(b)  the contact details of the data protection officer;	(b)  the contact details of the data protection officer;	
(c)  the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;	(c)  the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;	(c)  the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;	



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
(d) the categories of personal data concerned;	(d) the categories of personal data concerned;	(d) the categories of personal data concerned;	
(e) the recipients or categories of recipients of the personal data, if any;	(e) the recipients or categories of recipients of the personal data, if any;	(e) the recipients or categories of recipients of the personal data, if any;	
(f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 49, reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.	(f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 49, reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.	(f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 49, reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.	
2. In addition to the information	2. In addition to the information	2. In addition to the information	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
referred to in paragraph 1, the controller shall provide the data subject with the following further information necessary to ensure fair and transparent processing in respect of the data subject:	referred to in paragraph 1, the controller shall provide the data subject with the following further information necessary to ensure fair and transparent processing in respect of the data subject:	referred to in paragraph 1, the controller shall provide the data subject with the following further information necessary to ensure fair and transparent processing in respect of the data subject:	
(a)  the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;	(a)  the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;	(a)  the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;	
(b)  the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or, where applicable, the right to object to processing or the right to data portability;	(b)  the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or, where applicable, the right to object to processing or the right to data portability;	(b)  the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or, where applicable, the right to object to processing or the right to data portability;	
(c)  where the processing is based on point (d) of Article 5(1) or point (a) of Article 10(2), the existence of the	(c)  where the processing is based on point (d) of Article 5(1) or point (a) of Article 10(2), the existence of the	(c)  where the processing is based on point (d) of Article 5(1) or point (a) of Article 10(2), the existence of	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;	right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;	the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;	
(d)  the right to lodge a complaint with the European Data Protection Supervisor;	(d)  the right to lodge a complaint with the European Data Protection Supervisor;	(d)  the right to lodge a complaint with the European Data Protection Supervisor;	
(e)  from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;	(e)  from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;	(e)  from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;	
(f)  the existence of automated decision-making, including profiling, referred to in Article 24 (1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.	(f)  the existence of automated decision-making, including profiling, referred to in Article 24 (1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.	(f)  the existence of automated decision-making, including profiling, referred to in Article 24 (1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
3.  The controller shall provide the information referred to in paragraphs 1 and 2;	3.  The controller shall provide the information referred to in paragraphs 1 and 2;	3.  The controller shall provide the information referred to in paragraphs 1 and 2;	
(a)  within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;	(a)  within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;	(a)  within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;	
(b)  if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or	(b)  if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or	(b)  if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or	
(c)  if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.	(c)  if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.	(c)  if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>4.</p> <p>Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.</p>	<p>4.</p> <p>Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.</p>	<p>4.</p> <p>Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.</p>	
<p>5.</p> <p>Paragraphs 1 to 4 shall not apply where and insofar as:</p>	<p>5.</p> <p>Paragraphs 1 to 4 shall not apply where and insofar as:</p>	<p>5.</p> <p>Paragraphs 1 to 4 shall not apply where and insofar as:</p>	
<p>(a)</p> <p>the data subject already has the information;</p>	<p>(a)</p> <p>the data subject already has the information;</p>	<p>(a)</p> <p>the data subject already has the information;</p>	
<p>(b)</p> <p>the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for</p>	<p>(b)</p> <p>the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for</p>	<p>(b)</p> <p>the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
archiving purposes in the public interest, scientific or historical research purposes or statistical purposes or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing;	archiving purposes in the public interest, scientific or historical research purposes or statistical purposes or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing.	archiving purposes in the public interest, scientific or historical research purposes or statistical purposes or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing;	
(c)  obtaining or disclosure is expressly laid down by Union law; or	<b>AM 42</b>  (c)  obtaining or disclosure is expressly laid down by Union law <i>to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interest</i> ; or	(c)  obtaining or disclosure is expressly laid down by Union law, <b>which provides appropriate measures to protect the data subject's legitimate interests</b> ; or	(c) obtaining or disclosure is expressly laid down by Union law, which provides appropriate measures to protect the data subject's legitimate interests; or
(d)  where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union law.	<b>AM 43</b>  (d)  where the <i>personal</i> data must remain confidential subject to an obligation of professional secrecy regulated by Union law, <i>including a statutory obligation of secrecy</i> .	(d)  where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union law.	(d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union law, including a statutory obligation of secrecy.

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<b>AM 44</b> <b>5a.</b> <i>In the cases referred to in paragraph 5(b) the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interest, including making the information publicly available.</i>		5a. In the cases referred to in paragraph 5(b) the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interest, including making the information publicly available.
<i>Article 17</i>	<i>Article 17</i>	<i>Article 17</i>	
<i>Right of access by the data subject</i>	<i>Right of access by the data subject</i>	<i>Right of access by the data subject</i>	
1.  The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:	1.  The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:	1.  The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:	
(a)  the purposes of the processing;	(a)  the purposes of the processing;	(a)  the purposes of the processing;	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
(b) the categories of personal data concerned;	(b) the categories of personal data concerned;	(b) the categories of personal data concerned;	
(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;	(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;	(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;	
(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;	(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;	(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;	
(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;	(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;	(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such	



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
		processing;	
(f) the right to lodge a complaint with the European Data Protection Supervisor;	(f) the right to lodge a complaint with the European Data Protection Supervisor;	(f) the right to lodge a complaint with the European Data Protection Supervisor;	
(g) where the personal data are not collected from the data subject, any available information as to their source;	(g) where the personal data are not collected from the data subject, any available information as to their source;	(g) where the personal data are not collected from the data subject, any available information as to their source;	
(h) the existence of automated decision-making, including profiling, referred to in Article 24(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.	(h) the existence of automated decision-making, including profiling, referred to in Article 24(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.	(h) the existence of automated decision-making, including profiling, referred to in Article 24(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.	
2.	2.	2.	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 49 relating to the transfer.	Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 49 relating to the transfer.	Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 49 relating to the transfer.	
3.  The controller shall provide a copy of the personal data undergoing processing. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.	3.  The controller shall provide a copy of the personal data undergoing processing. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.	3.  The controller shall provide a copy of the personal data undergoing processing. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.	
4.  The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.	4.  The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.	4.  The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.	
<b>SECTION 3</b> <b>RECTIFICATION AND</b>	<b>SECTION 3</b> <b>RECTIFICATION AND</b>	<b>SECTION 3</b> <b>RECTIFICATION AND</b>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
ERASURE	ERASURE	ERASURE	
<i>Article 18</i>	<i>Article 18</i>	<i>Article 18</i>	
<i>Right to rectification</i>	<i>Right to rectification</i>	<i>Right to rectification</i>	
The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.	The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.	The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.	
<i>Article 19</i>	<i>Article 19</i>	<i>Article 19</i>	
<i>Right to erasure ('right to be forgotten')</i>	<i>Right to erasure ('right to be forgotten')</i>	<i>Right to erasure ('right to be forgotten')</i>	
1.  The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the	1.  The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the	1.  The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
obligation to erase personal data without undue delay where one of the following grounds applies:	obligation to erase personal data without undue delay where one of the following grounds applies:	shall have the obligation to erase personal data without undue delay where one of the following grounds applies:	
(a)  the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;	(a)  the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;	(a)  the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;	
(b)  the data subject withdraws consent on which the processing is based according to point (d) of Article 5(1), or point (a) of Article 10(2), and where there is no other legal ground for the processing;	(b)  the data subject withdraws consent on which the processing is based according to point (d) of Article 5(1), or point (a) of Article 10(2), and where there is no other legal ground for the processing;	(b)  the data subject withdraws consent on which the processing is based according to point (d) of Article 5(1), or point (a) of Article 10(2), and where there is no other legal ground for the processing;	
(c)  the data subject objects to the processing pursuant to Article 23(1) and there are no overriding legitimate grounds for the processing;	(c)  the data subject objects to the processing pursuant to Article 23(1) and there are no overriding legitimate grounds for the processing;	(c)  the data subject objects to the processing pursuant to Article 23(1) and there are no overriding legitimate grounds for the processing;	
(d)	(d)	(d)	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
the personal data have been unlawfully processed;	the personal data have been unlawfully processed;	the personal data have been unlawfully processed;	
(e) the personal data have to be erased for compliance with a legal obligation to which the controller is subject;	(e) the personal data have to be erased for compliance with a legal obligation to which the controller is subject;	(e) the personal data have to be erased for compliance with a legal obligation to which the controller is subject;	
(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).	(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).	(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).	
2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject	2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject	2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers, <b>or controllers other</b>	2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers, or controllers other than Union institutions and bodies, which are processing the

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.	has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.	<b>than Union institutions and bodies</b> , which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.	personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.
3.  Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:	3.  Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:	3.  Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:	
(a)  for exercising the right of freedom of expression and information;	(a)  for exercising the right of freedom of expression and information;	(a)  for exercising the right of freedom of expression and information;	
(b)  for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;	(b)  for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;	(b)  for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;	
(c)	(c)	(c)	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 10(2) as well as Article 10(3);	for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 10(2) as well as Article 10(3);	for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 10(2) as well as Article 10(3);	
(d)  for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or	(d)  for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or	(d)  for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or	
(e)  for the establishment, exercise or defence of legal claims.	(e)  for the establishment, exercise or defence of legal claims.	(e)  for the establishment, exercise or defence of legal claims.	
<i>Article 20</i>	<i>Article 20</i>	<i>Article 20</i>	
<i>Right to restriction of processing</i>	<i>Right to restriction of processing</i>	<i>Right to restriction of processing</i>	
1.  The data subject shall have the right to obtain from the controller restriction of processing where one	1.  The data subject shall have the right to obtain from the controller	1.  The data subject shall have the right to obtain from the controller	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
of the following applies:	restriction of processing where one of the following applies:	restriction of processing where one of the following applies:	
(a)  the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy, including the completeness, of the personal data;	(a)  the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy, including the completeness, of the personal data;	(a)  the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy, including the completeness, of the personal data;	
(b)  the processing is unlawful and the data subject opposes their erasure and requests the restriction of their use instead;	<b>AM 45</b>  (b)  the processing is unlawful and the data subject opposes <del>their</del> <i>the</i> erasure <b>of the personal data</b> and requests the restriction of their use instead;	(b)  the processing is unlawful and the data subject opposes <del>their</del> erasure <b>of the personal data</b> and requests the restriction of their use instead;	(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
(c)  the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;	(c)  the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;	(c)  the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;	



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>(d)</p> <p>the data subject has objected to processing pursuant to Article 23(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.</p>	<p>(d)</p> <p>the data subject has objected to processing pursuant to Article 23(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.</p>	<p>(d)</p> <p>the data subject has objected to processing pursuant to Article 23(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.</p>	
<p>2.</p> <p>Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.</p>	<p>2.</p> <p>Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.</p>	<p>2.</p> <p>Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
3.  A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.	3.  A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.	3.  A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.	
4.  In automated filing systems restriction of processing shall in principle be ensured by technical means. The fact that the personal data are restricted shall be indicated in the system in such a way that it becomes clear that the personal data may not be used.	4.  In automated filing systems restriction of processing shall in principle be ensured by technical means. The fact that the personal data are restricted shall be indicated in the system in such a way that it becomes clear that the personal data may not be used.	4.  In automated filing systems restriction of processing shall in principle be ensured by technical means. The fact that the personal data are restricted shall be indicated in the system in such a way that it becomes clear that the personal data may not be used.	
<i>Article 21</i>	<i>Article 21</i>	<i>Article 21</i>	
<i>Notification obligation regarding rectification or erasure of personal data or restriction of processing</i>	<i>Notification obligation regarding rectification or erasure of personal data or restriction of processing</i>	<i>Notification obligation regarding rectification or erasure of personal data or restriction of processing</i>	
The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in	The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance	The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
accordance with Article 18, Article 19(1) and Article 20 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.	with Article 18, Article 19(1) and Article 20 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.	accordance with Article 18, Article 19(1) and Article 20 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.	
<i>Article 22</i>	<i>Article 22</i>	<i>Article 22</i>	
<i>Right to data portability</i>	<i>Right to data portability</i>	<i>Right to data portability</i>	
1.  The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:	1.  The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:	1.  The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:	
(a)	(a)	(a)	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
the processing is based on consent pursuant to point (d) of Article 5(1) or point (a) of Article 10(2) or on a contract pursuant to point (c) of Article 5(1); and	the processing is based on consent pursuant to point (d) of Article 5(1) or point (a) of Article 10(2) or on a contract pursuant to point (c) of Article 5(1); and	the processing is based on consent pursuant to point (d) of Article 5(1) or point (a) of Article 10(2) or on a contract pursuant to point (c) of Article 5(1); and	
(b)  the processing is carried out by automated means.	(b)  the processing is carried out by automated means.	(b)  the processing is carried out by automated means.	
2.  In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.	2.  In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.	2.  In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another <b>or to controllers other than Union institutions and bodies</b> , where technically feasible.	2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another or to controllers other than Union institutions and bodies, where technically feasible.
3.  The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 19. That right shall not apply to processing necessary for the	3.  The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 19. That right shall not apply to processing necessary for the	3.  The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 19. That right shall not apply to processing necessary for the	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.	performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.	performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.	
4.  The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.	4.  The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.	4.  The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.	
<b>SECTION 4</b>  <b>RIGHT TO OBJECT AND AUTOMATED INDIVIDUAL DECISION-MAKING</b>	<b>SECTION 4</b>  <b>RIGHT TO OBJECT AND AUTOMATED INDIVIDUAL DECISION-MAKING</b>	<b>SECTION 4</b>  <b>RIGHT TO OBJECT AND AUTOMATED INDIVIDUAL DECISION-MAKING</b>	
<i>Article 23</i>	<i>Article 23</i>	<i>Article 23</i>	
<i>Right to object</i>	<i>Right to object</i>	<i>Right to object</i>	
1.  The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is	1.  The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is	1.  The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
based on point (a) of Article 5(1), including profiling based on that provision. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.	based on point (a) of Article 5(1), including profiling based on that provision. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.	is based on point (a) of Article 5(1), including profiling based on that provision. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.	
2.  At the latest at the time of the first communication with the data subject, the right referred to in paragraph 1 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.	2.  At the latest at the time of the first communication with the data subject, the right referred to in paragraph 1 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.	2.  At the latest at the time of the first communication with the data subject, the right referred to in paragraph 1 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.	
3.  Without prejudice to Articles 34 and 35, in the context of the use of information society services the data subject may exercise his or her right to object by automated means using	3.  Without prejudice to Articles 34 and 35, in the context of the use of information society services the data subject may exercise his or her right to object by automated means using	3.  Without prejudice to Articles 34 and 35, in the context of the use of information society services the data subject may exercise his or her right to object by automated	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
technical specifications.	technical specifications.	means using technical specifications.	
<p>4.</p> <p>Where personal data are processed for scientific or historical research purposes or statistical purposes, the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.</p>	<p>4.</p> <p>Where personal data are processed for scientific or historical research purposes or statistical purposes, the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.</p>	<p>4.</p> <p>Where personal data are processed for scientific or historical research purposes or statistical purposes, the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.</p>	
<i>Article 24</i>	<i>Article 24</i>	<i>Article 24</i>	
<i>Automated individual decision-making, including profiling</i>	<i>Automated individual decision-making, including profiling</i>	<i>Automated individual decision-making, including profiling</i>	
<p>1.</p> <p>The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him</p>	<p>1.</p> <p>The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him</p>	<p>1.</p> <p>The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
or her.	or her.	significantly affects him or her.	
2.  Paragraph 1 shall not apply if the decision:	2.  Paragraph 1 shall not apply if the decision:	2.  Paragraph 1 shall not apply if the decision:	
(a)  is necessary for entering into, or performance of, a contract between the data subject and the controller;	(a)  is necessary for entering into, or performance of, a contract between the data subject and the controller;	(a)  is necessary for entering into, or performance of, a contract between the data subject and the controller;	
(b)  is authorised by Union law, which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or	(b)  is authorised by Union law, which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or	(b)  is authorised by Union law, which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or	
(c)  is based on the data subject's explicit consent.	(c)  is based on the data subject's explicit consent.	(c)  is based on the data subject's explicit consent.	
3.  In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable	3.  In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable	3.  In the cases referred to in points (a) and (c) of paragraph 2, the data	



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.	measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.	controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>4.</p> <p>Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 10(1), unless point (a) or (g) of Article 10(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.</p>	<p>4.</p> <p>Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 10(1), unless point (a) or (g) of Article 10(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.</p>	<p>4.</p> <p>Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 10(1), unless point (a) or (g) of Article 10(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.</p>	
<b>SECTION 5</b>	<b>SECTION 5</b>	<b>SECTION 5</b>	
<b>RESTRICTIONS</b>	<b>RESTRICTIONS</b>	<b>RESTRICTIONS</b>	
<i>Article 25</i>	<i>Article 25</i>	<i>Article 25</i>	
<i>Restrictions</i>	<i>Restrictions</i>	<i>Restrictions</i>	
<p>1.</p> <p>Legal acts adopted on the basis of the Treaties or, in matters relating to the operation of the Union institutions and bodies, internal rules laid down by the latter may restrict the application of Articles 14 to 22, 34 and 38, as well as Article 4 in so far as its</p>	<p><b>AM 46</b></p> <p>1.</p> <p>Legal acts adopted on the basis of the Treaties or, in matters relating to the operation of the Union institutions and bodies, internal rules laid down by the latter may restrict the application of Articles</p>	<p>1.</p> <p>Legal acts adopted on the basis of the Treaties or, in matters relating to the operation of the Union institutions and bodies, internal rules laid down by the latter may restrict the application of Articles 14 to 22, 34 and 38, as</p>	<p>Council suggestion:</p> <p>1.</p> <p>Legal acts adopted on the basis of the Treaties or, in matters relating to the operation of the Union institutions and bodies, internal rules laid down by the latter may restrict the application of</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
provisions correspond to the rights and obligations provided for in Articles 14 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:	14 to 22, <del>34</del> and 38, as well as Article 4 in so far as its provisions correspond to the rights and obligations provided for in Articles 14 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:	well as Article 4 in so far as its provisions correspond to the rights and obligations provided for in Articles 14 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:	Articles 14 to 22, 34 and 38, as well as Article 4 in so far as its provisions correspond to the rights and obligations provided for in Articles 14 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:
(a)  the national security, public security or defence of the Member States;	(a)  the national security, public security or defence of the Member States;	(a)  the national security, public security or defence of the Member States;	
(b)  the prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;	(b)  the prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;	(b)  the prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;	
(c)  other important objectives of	(c)  <del>other important objectives of</del>	(c)  other important objectives of	(c)  other important objectives of

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;	general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;	general public interest of the Union or of a Member State, in particular <b>the objectives of the common foreign and security policy of the Union</b> or an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;	general public interest of the Union or of a Member State, in particular the objectives of the common foreign and security policy of the Union or an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;
(d) the internal security of Union institutions and bodies, including of their electronic communication networks;	(d) the internal security of Union institutions and bodies, including of their electronic communication networks;	(d) the internal security of Union institutions and bodies, including of their electronic communications networks;	
(e) the protection of judicial independence and judicial proceedings;	(e) the protection of judicial independence and judicial proceedings;	(e) the protection of judicial independence and judicial proceedings;	
(f) the prevention, investigation, detection and prosecution of breaches of ethics for regulated	(f) the prevention, investigation, detection and prosecution of breaches of ethics for regulated	(f) the prevention, investigation, detection and prosecution of breaches of ethics for regulated	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
professions;	professions;	professions;	
(g) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (c).	(g) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (c).	(g) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (c).	
(h) the protection of the data subject or the rights and freedoms of others;	(h) the protection of the data subject or the rights and freedoms of others;	(h) the protection of the data subject or the rights and freedoms of others;	
(i) the enforcement of civil law claims.	(i) the enforcement of civil law claims.	(i) the enforcement of civil law claims.	
	<b>AM 47</b>  <i>1a.</i>  <i>Acts adopted under paragraph 1 shall be clear and precise. Their application shall be foreseeable to persons subject to it.</i>		Council suggestion: deletion
	<b>AM 48</b>		Council suggestion: deletion

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<p>AM 48</p> <p><i>1b.</i></p> <p><i>In particular, any legal act adopted under paragraph 1 shall contain specific provisions at least, where relevant, as to:</i></p>		
	<i>(a) the purposes of the processing or categories of processing;</i>		
	<i>(b) the categories of personal data;</i>		
	<i>(c) the scope of the restriction introduced;</i>		
	<i>(d) the safeguards to prevent abuse or unlawful access or transfer;</i>		
	<i>(e) the specification of the controller or categories of controllers;</i>		
	<i>(f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;</i>		

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>(g) the risks to the rights and freedoms of data subjects; and</i>		
	<i>(h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.</i>		

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>2.</p> <p>Where a restriction is not provided for by a legal act adopted on the basis of the Treaties or by an internal rule in accordance with paragraph 1, the Union institutions and bodies may restrict the application of Articles 14 to 22, 34 and 38, as well as Article 4 in so far as its provisions correspond to the rights and obligations provided for in Articles 14 to 22, if such a restriction respects the essence of the fundamental rights and freedoms, in relation to a specific processing operation, and is a necessary and proportionate measure in a democratic society to safeguard one or more of the objectives referred to in paragraph 1. The restriction shall be notified to the competent data protection officer.</p>	<p>AM 49</p> <p><del>2.</del></p> <p><i><del>Where a restriction is not provided for by a legal act adopted on the basis of the Treaties or by an internal rule in accordance with paragraph 1, the Union institutions and bodies may restrict the application of Articles 14 to 22, 34 and 38, as well as Article 4 in so far as its provisions correspond to the rights and obligations provided for in Articles 14 to 22, if such a restriction respects the essence of the fundamental rights and freedoms, in relation to a specific processing operation, and is a necessary and proportionate measure in a democratic society to safeguard one or more of the objectives referred to in paragraph 1. The restriction shall be notified to the competent data protection officer.</del></i></p>	<p><del>2.</del></p> <p><del>Where a restriction is not provided for by a legal act adopted on the basis of the Treaties or by an internal rule in accordance with paragraph 1, the Union institutions and bodies may restrict the application of Articles 14 to 22, 34 and 38, as well as Article 4 in so far as its provisions correspond to the rights and obligations provided for in Articles 14 to 22, if such a restriction respects the essence of the fundamental rights and freedoms, in relation to a specific processing operation, and is a necessary and proportionate measure in a democratic society to safeguard one or more of the objectives referred to in paragraph 1. The restriction shall be notified to the competent data protection officer.</del></p>	<p>deletion</p>



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
		<b>2a</b>  <b>In particular, any legal act or internal rule referred to in paragraph 1 shall contain specific provisions, where relevant, as to:</b>	Council suggestion:  2a  In particular, any legal act or internal rule referred to in paragraph 1 shall contain specific provisions, where relevant, as to:
		<b>(a)</b>  <b>the purposes of the processing or categories of processing;</b>	(a)  the purposes of the processing or categories of processing;
		<b>(b)</b>  <b>the categories of personal data;</b>	(b)  the categories of personal data;
		<b>(c)</b>  <b>the scope of the restrictions introduced;</b>	(c)  the scope of the restrictions introduced;
		<b>(d)</b>  <b>the safeguards to prevent abuse or unlawful access or transfer;</b>	(d)  the safeguards to prevent abuse or unlawful access or transfer;
		<b>(e)</b>	(e)

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
		<b>the specifications of the controller or categories of controllers;</b>	the specifications of the controller or categories of controllers;
		(f)  <b>the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing; and</b>	(f)  the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing; and
		(g)  <b>the risks to the rights and freedoms of data subjects.</b>	(g)  The risks to the rights and freedoms of data subjects.
3.  Where personal data are processed for scientific or historical research purposes or statistical purposes, Union law, which may include internal rules, may provide for derogations from the rights referred to in Articles 17, 18, 20 and 23 subject to the conditions and <del>safeguards</del> referred to in Article 13 in so far as such rights are likely to	<b>AM 50</b>  3.  Where personal data are processed for scientific or historical research purposes or statistical purposes, Union law, <del>which may include internal rules,</del> may provide for derogations from the rights referred to in Articles 17, 18, 20 and 23 subject to the conditions and	3.  Where personal data are processed for scientific or historical research purposes or statistical purposes, Union law, which may include internal-rules <b>adopted by Union institutions and bodies in matters relating to their operation</b> , may provide for derogations from the rights referred to in Articles 17, 18, 20 and 23 subject to the conditions	Council suggestion:  3.  Where personal data are processed for scientific or historical research purposes or statistical purposes, Union law, which may include internal-rules adopted by Union institutions and bodies in matters relating to their operation, may provide for derogations from the

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.	safeguards referred to in Article 13 in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.	and safeguards referred to in Article 13 in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.	rights referred to in Articles 17, 18, 20 and 23 subject to the conditions and safeguards referred to in Article 13 in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.
<p>4.</p> <p>Where personal data are processed for archiving purposes in the public interest, Union law, which may include internal rules, may provide for derogations from the rights referred to in Articles 17, 18, 20, 21, 22 and 23 subject to the conditions and safeguards referred to in Article 13 in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.</p>	<p><b>AM 51</b></p> <p>4.</p> <p>Where personal data are processed for archiving purposes in the public interest, Union law, <del>which may include internal rules,</del> may provide for derogations from the rights referred to in Articles 17, 18, 20, 21, 22 and 23 subject to the conditions and safeguards referred to in Article 13 in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.</p>	<p>4.</p> <p>Where personal data are processed for archiving purposes in the public interest, Union law, which may include internal rules <b>adopted by Union institutions and bodies in matters relating to their operation</b>, may provide for derogations from the rights referred to in Articles 17, 18, 20, 21, 22 and 23 subject to the conditions and safeguards referred to in Article 13 in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of</p>	<p>Council suggestion:</p> <p>4.</p> <p>Where personal data are processed for archiving purposes in the public interest, Union law, which may include internal rules adopted by Union institutions and bodies in matters relating to their operation, may provide for derogations from the rights referred to in Articles 17, 18, 20, 21, 22 and 23 subject to the conditions and safeguards referred to in Article 13 in so far as such rights are likely to render impossible or seriously impair the achievement of the specific</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
		those purposes.	purposes, and such derogations are necessary for the fulfilment of those purposes.
<p>5.</p> <p>Internal rules referred to in paragraphs 1, 3 and 4 shall be sufficiently clear and precise and subject to appropriate publication.</p>	<p><b>AM 52</b></p> <p><del>5.</del>  <del>Internal rules referred to in paragraphs 1, 3 and 4 shall be sufficiently clear and precise and subject to appropriate publication.</del></p>	<p>5.</p> <p>Internal rules referred to in paragraphs 1, 3 and 4 shall be <b>sufficiently</b> clear and precise <b>acts of general application, intended to produce legal effects vis-a-vis data subjects, adopted at the highest level of management of the Union institutions and bodies</b> and subject to <b>appropriate</b> publication <b>in the Official Journal of the European Union.</b></p>	<p>Council suggestion:</p> <p>5.</p> <p>Internal rules referred to in paragraphs 1, 3 and 4 shall be clear and precise acts of general application, intended to produce legal effects vis-a-vis data subjects, adopted at the highest level of management of the Union institutions and bodies and subject to publication in the Official Journal of the European Union.</p>
<p>6.</p> <p>If a restriction is imposed pursuant to paragraphs 1 or 2, the data subject shall be informed, in accordance with Union law, of the principal reasons on which the application of the restriction is based and of his or her right to lodge a complaint with the European Data Protection</p>	<p><b>AM 53</b></p> <p>6.</p> <p>If a restriction is imposed pursuant to paragraphs 1 <del>or 2</del>, the data subject shall be informed, in accordance with Union law, of the principal reasons on which the application of the restriction is based and of his or her right to lodge a complaint with the</p>	<p>6.</p> <p>If a restriction is imposed pursuant to paragraphs 1 or 2, the data subject shall be informed, in accordance with Union law, of the principal reasons on which the application of the restriction is based and of his or her right to lodge a complaint with the European Data Protection</p>	<p>6.</p> <p>If a restriction is imposed pursuant to paragraph 1 the data subject shall be informed, in accordance with Union law, of the principal reasons on which the application of the restriction is based and of his or her right to lodge a complaint with the European Data Protection</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
Supervisor.	European Data Protection Supervisor.	Supervisor.	Supervisor.
<p>7.</p> <p>If a restriction imposed pursuant to paragraphs 1 or 2 is relied upon to deny access to the data subject, the European Data Protection Supervisor shall, when investigating the complaint, only inform him or her of whether the data have been processed correctly and, if not, whether any necessary corrections have been made.</p>	<p><b>AM 54</b></p> <p>7.</p> <p>If a restriction imposed pursuant to paragraphs 1 <del>or 2</del> is relied upon to deny access to the data subject, the European Data Protection Supervisor shall, when investigating the complaint, only inform him or her of whether the data have been processed correctly and, if not, whether any necessary corrections have been made.</p>	<p>7.</p> <p>If a restriction imposed pursuant to paragraphs 1 or 2 is relied upon to deny access to the data subject, the European Data Protection Supervisor shall, when investigating the complaint, only inform him or her of whether the data have been processed correctly and, if not, whether any necessary corrections have been made.</p>	<p>7.</p> <p>If a restriction imposed pursuant to paragraph 1 is relied upon to deny access to the data subject, the European Data Protection Supervisor shall, when investigating the complaint, only inform him or her of whether the data have been processed correctly and, if not, whether any necessary corrections have been made.</p>
<p>8.</p> <p>Provision of the information referred to in paragraphs 6 and 7 and in Article 46(2) may be deferred, omitted or denied if it would cancel the effect of the restriction imposed pursuant to paragraph 1 or 2.</p>	<p><b>AM 55</b></p> <p>8.</p> <p>Provision of the information referred to in paragraphs 6 and 7 and in Article 46(2) may be deferred, omitted or denied if it would cancel the effect of the restriction imposed pursuant to paragraph 1 <del>or 2</del>.</p>	<p>8.</p> <p>Provision of the information referred to in paragraphs 6 and 7 and in Article 46(2) may be deferred, omitted or denied if it would cancel the effect of the restriction imposed pursuant to paragraph 1 or 2.</p>	<p>8.</p> <p>Provision of the information referred to in paragraphs 6 and 7 and in Article 46(2) may be deferred, omitted or denied if it would cancel the effect of the restriction imposed pursuant to paragraph 1.</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<b>CHAPTER IV</b> <b>CONTROLLER AND</b> <b>PROCESSOR</b>	<b>CHAPTER IV</b> <b>CONTROLLER AND</b> <b>PROCESSOR</b>	<b>CHAPTER IV</b> <b>CONTROLLER AND</b> <b>PROCESSOR</b>	
<b>SECTION 1</b> <b>GENERAL</b> <b>OBLIGATIONS</b>	<b>SECTION 1</b> <b>GENERAL</b> <b>OBLIGATIONS</b>	<b>SECTION 1</b> <b>GENERAL</b> <b>OBLIGATIONS</b>	
<i>Article 26</i>	<i>Article 26</i>	<i>Article 26</i>	
<i>Responsibility of the controller</i>	<i>Responsibility of the controller</i>	<i>Responsibility of the controller</i>	
1.  Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those <del>measures</del> shall be reviewed	1.  Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed	1.  Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
and updated where necessary.	and updated where necessary.	be reviewed and updated where necessary.	
2.  Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.	2.  Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.	2.  Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.	
	<b>AM 56</b>  <b>2a.</b>  <i>Adherence to approved certification mechanisms as referred to in Article 42 of Regulation (EU) 2016/679 may be used as an element by which to demonstrate compliance with the obligations of the controller.</i>		2a. Adherence to approved certification mechanisms as referred to in Article 42 of Regulation (EU) 2016/679 may be used as an element by which to demonstrate compliance with the obligations of the controller.

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<i>Article 27</i>	<i>Article 27</i>	<i>Article 27</i>	
<i>Data protection by design and by default</i>	<i>Data protection by design and by default</i>	<i>Data protection by design and by default</i>	
<p>1.</p> <p>Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.</p>	<p>1.</p> <p>Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.</p>	<p>1.</p> <p>Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data</p>	



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
		subjects.	
<p>2.</p> <p>The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.</p>	<p>2.</p> <p>The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.</p>	<p>2.</p> <p>The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.</p>	
	<p><b>AM 57</b></p> <p><b>2a.</b></p> <p><i>An approved certification mechanism pursuant to Article 42 of Regulation (EU) 2016/679 may be used as an element to</i></p>		<p>2a. An approved certification mechanism pursuant to Article 42 of Regulation (EU) 2016/679 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.</i>		

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<i>Article 28</i>	<i>Article 28</i>	<i>Article 28</i>	
<i>Joint controllers</i>	<i>Joint controllers</i>	<i>Joint controllers</i>	
<p>1.</p> <p>Where a Union institution or body together with one or more controllers, which may be Union institutions or bodies or not, jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with their data protection obligations, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 15 and 16, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a</p>	<p>1.</p> <p>Where a Union institution or body together with one or more controllers, which may be Union institutions or bodies or not, jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with their data protection obligations, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 15 and 16, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a</p>	<p>1.</p> <p>Where a <b>controller, jointly with one or more controllers or controllers other than Union institutions and bodies, Union institution or body together with one or more controllers, which may be Union institutions or bodies or not, jointly</b> determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with their data protection obligations, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 15 and 16, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the <b>joint</b> controllers are determined by</p>	<p>1. Where a controller, jointly with one or more controllers or controllers other than Union institutions and bodies, determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with their data protection obligations, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 15 and 16, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the joint controllers are determined by Union or Member State law to which the joint controllers are subject. The arrangement may designate a contact point for data subjects.</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
contact point for data subjects.	contact point for data subjects.	Union or Member State law to which the <b>joint</b> controllers are subject. The arrangement may designate a contact point for data subjects.	
2.  The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.	2.  The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.	2.  The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.	
3.  The data subject may exercise his or her rights under this Regulation in respect of and against one or more of the joint controllers, taking into account their roles as determined in the terms of the <del>arrangement</del> referred to in paragraph 1.	<b>AM 58</b>  3.  <i>I</i> <b><i>Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against one or more each of the joint controllers, taking into account their roles as determined in the terms of the arrangement referred to in paragraph 1.</i></b>	3.  The data subject may exercise his or her rights under this Regulation in respect of and against one or more of the joint controllers, taking into account their roles as determined in the terms of the arrangement referred to in paragraph 1.	3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<i>Article 29</i>	<i>Article 29</i>	<i>Article 29</i>	
<i>Processor</i>	<i>Processor</i>	<i>Processor</i>	
<p>1.</p> <p>Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.</p>	<p>1.</p> <p>Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.</p>	<p>1.</p> <p>Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.</p>	
<p>2.</p> <p>The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the</p>	<p>2.</p> <p>The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the</p>	<p>2.</p> <p>The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
controller the opportunity to object to such changes.	controller the opportunity to object to such changes.	controller the opportunity to object to such changes.	
<p>3.</p> <p>Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:</p>	<p>3.</p> <p>Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:</p>	<p>3.</p> <p>Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:</p>	
<p>(a)</p> <p>processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in</p>	<p>(a)</p> <p>processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in</p>	<p>(a)</p> <p>processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;	such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;	such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;	
(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;	(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;	(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;	
(c) takes all measures required pursuant to Article 33;	(c) takes all measures required pursuant to Article 33;	(c) takes all measures required pursuant to Article 33;	
(d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;	(d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;	(d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;	
(e) taking into account the nature of the processing, assists the controller by	(e) taking into account the nature of the processing, assists the controller by	(e) taking into account the nature of the processing, assists the	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;	appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;	controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;	
(f)  assists the controller in ensuring compliance with the obligations pursuant to Articles 33 to 40 taking into account the nature of processing and the information available to the processor;	(f)  assists the controller in ensuring compliance with the obligations pursuant to Articles 33 to 40 taking into account the nature of processing and the information available to the processor;	(f)  assists the controller in ensuring compliance with the obligations pursuant to Articles 33 to 40 taking into account the nature of processing and the information available to the processor;	
(g)  at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;	(g)  at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;	(g)  at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;	
(h)	(h)	(h)	



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.	makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.	makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.	
With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.	With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.	With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.	
4.  Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or	4.  Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or	4.  Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this	other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this	contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this	
Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.	Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.	Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.	
5.  When a processor is not a Union institution or body, its adherence to an approved code of conduct referred to in Article 40(5) of Regulation (EU) 2016/679 or an approved certification mechanism referred to in Article 42 of Regulation (EU) 2016/679 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of	5.  When a processor is not a Union institution or body, its adherence to an approved code of conduct referred to in Article 40(5) of Regulation (EU) 2016/679 or an approved certification mechanism referred to in Article 42 of Regulation (EU) 2016/679 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of	5.  When a processor is not a Union institution or body, its adherence to an approved code of conduct referred to in Article 40(5) of Regulation (EU) 2016/679 or an approved certification mechanism referred to in Article 42 of Regulation (EU) 2016/679 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
this Article.	this Article.	of this Article.	
<p>6.</p> <p>Without prejudice to any individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the processor other than a Union institution or body pursuant to Article 42 of Regulation (EU) 2016/679.</p>	<p>6.</p> <p>Without prejudice to any individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the processor other than a Union institution or body pursuant to Article 42 of Regulation (EU) 2016/679.</p>	<p>6.</p> <p>Without prejudice to any individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the processor other than a Union institution or body pursuant to Article 42 of Regulation (EU) 2016/679.</p>	
<p>7.</p> <p>The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 70(2).</p>	<p>7.</p> <p>The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 70(2).</p>	<p>7.</p> <p>The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 70(2).</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
8.  The European Data Protection Supervisor may adopt standard contractual clauses for the matters referred to in paragraphs 3 and 4.	8.  The European Data Protection Supervisor may adopt standard contractual clauses for the matters referred to in paragraphs 3 and 4.	8.  The European Data Protection Supervisor may adopt standard contractual clauses for the matters referred to in paragraphs 3 and 4.	
9.  The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.	9.  The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.	9.  The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.	
10.  Without prejudice to Articles 65 and 66, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.	10.  Without prejudice to Articles 65 and 66, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.	10.  Without prejudice to Articles 65 and 66, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.	
<i>Article 30</i>	<i>Article 30</i>	<i>Article 30</i>	
<i>Processing under the authority of the controller and processor</i>	<i>Processing under the authority of the controller and processor</i>	<i>Processing under the authority of the controller and processor</i>	
The processor and any person	The processor and any person acting	The processor and any person	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.	under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.	acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.	
<i>Article 31</i>	<i>Article 31</i>	<i>Article 31</i>	
<i>Records of processing activities</i>	<i>Records of processing activities</i>	<i>Records of processing activities</i>	
1.  Each controller shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:	1.  Each controller shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:	1.  Each controller shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:	
(a)  the name and contact details of the controller, the data protection officer and, where applicable, the processor and the joint controller;	(a)  the name and contact details of the controller, the data protection officer and, where applicable, the processor and the joint controller;	(a)  the name and contact details of the controller, the data protection officer and, where applicable, the processor and the joint controller;	
(b)  the purposes of the processing;	(b)  the purposes of the processing;	(b)  the purposes of the processing;	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
(c) description of the categories of data subjects and of the categories of personal data;	(c) description of the categories of data subjects and of the categories of personal data;	(c) a description of the categories of data subjects and of the categories of personal data;	
(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in Member States, third countries or international organisations;	(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in Member States, third countries or international organisations;	(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in Member States, third countries or international organisations;	
(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards;	(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards;	(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards;	
(f) where possible, the envisaged time limits for erasure of the different	(f) where possible, the envisaged time limits for erasure of the different	(f) where possible, the envisaged time limits for erasure of the different	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
categories of data;	categories of data;	categories of data;	
(g)  where possible, a general description of the technical and organisational security measures referred to in Article 33.	(g)  where possible, a general description of the technical and organisational security measures referred to in Article 33.	(g)  where possible, a general description of the technical and organisational security measures referred to in Article 33.	
2.  Each processor shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:	2.  Each processor shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:	2.  Each processor shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:	
(a)  the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and of the data protection officer;	(a)  the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and of the data protection officer;	(a)  the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and of the data protection officer;	
(b)  the categories of processing carried out on behalf of each controller;	(b)  the categories of processing carried out on behalf of each controller;	(b)  the categories of processing carried out on behalf of each controller;	
(c)	(c)	(c)	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards;	where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards;	where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards;	
(d)  where possible, a general description of the technical and organisational security measures referred to in Article 33.	(d)  where possible, a general description of the technical and organisational security measures referred to in Article 33.	(d)  where possible, a general description of the technical and organisational security measures referred to in Article 33.	
3.  The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.	3.  The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.	3.  The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.	
4.  Union institutions and bodies shall make the record available to the European Data Protection Supervisor on request.	4.  Union institutions and bodies shall make the record available to the European Data Protection Supervisor on request.	4.  Union institutions and bodies shall make the record available to the European Data Protection Supervisor on request.	



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>5.</p> <p>Union institutions and bodies may decide to keep their records of processing activities in a central register. In this case, they may also decide to make the register publicly accessible.</p>	<p><b>AM 59</b></p> <p>5.</p> <p>Union institutions and bodies <del>may decide to</del> <b>shall</b> keep their records of processing activities in a central register. <del>In this case, they may also decide to</del> <b>and</b> make the register publicly accessible.</p>	<p>5.</p> <p>Union institutions and bodies may decide to keep their records of processing activities in a central register. In this case, they may also decide to make the register publicly accessible.</p>	<p>Council suggestion:</p> <p>5.</p> <p>Unless it is not appropriate taking into account the size of the institution or agency, Union institutions and bodies shall keep their records of processing activities in a central register. They shall make the register publicly accessible.</p>
<i>Article 32</i>	<i>Article 32</i>	<i>Article 32</i>	
<i>Co-operation with the European Data Protection Supervisor</i>	<i>Co-operation with the European Data Protection Supervisor</i>	<i>Co-operation with the European Data Protection Supervisor</i>	
Union institutions and bodies shall cooperate, on request, with the European Data Protection Supervisor in the performance of its tasks.	Union institutions and bodies shall cooperate, on request, with the European Data Protection Supervisor in the performance of its tasks.	Union institutions and bodies shall cooperate, on request, with the European Data Protection Supervisor in the performance of its tasks.	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<b>SECTION 2</b>  <b>SECURITY OF PERSONAL DATA AND CONFIDENTIALITY OF ELECTRONIC COMMUNICATIONS</b>	AM 60  <b>SECTION 2</b> <i>SECURITY OF PERSONAL DATA AND</i> <del>CONFIDENTIALITY OF ELECTRONIC COMMUNICATIONS</del>	<b>SECTION 2</b>  <b>SECURITY OF PERSONAL DATA AND CONFIDENTIALITY OF ELECTRONIC COMMUNICATIONS</b>	<b>SECTION 2</b>  <b>SECURITY OF PERSONAL DATA</b>
<i>Article 33</i>	<i>Article 33</i>	<i>Article 33</i>	
<i>Security of processing</i>	<i>Security of processing</i>	<i>Security of processing</i>	
1.  Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as	1.  Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as	1.  Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
appropriate:	appropriate:	appropriate:	
(a) the pseudonymisation and encryption of personal data;	(a) the pseudonymisation and encryption of personal data;	(a) the pseudonymisation and encryption of personal data;	
(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;	(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;	(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;	
(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;	(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;	(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;	
(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.	(d) process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.	a (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>2.</p> <p>In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.</p>	<p>2.</p> <p>In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.</p>	<p>2.</p> <p>In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.</p>	
<p>3.</p> <p>The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union law.</p>	<p>3.</p> <p>The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union law.</p>	<p>3.</p> <p>The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union law.</p>	
	<p><b>AM 61</b></p> <p><b>3a.</b></p> <p><i>Adherence to an approved certification mechanism as</i></p>		<p>3a. Adherence to an approved certification mechanism as referred to in Article 42 of Regulation (EU) 2016/679 may be used as an element by which to demonstrate compliance with the</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>referred to in Article 42 of Regulation (EU) 2016/679 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.</i>		requirements set out in paragraph 1 of this Article.
	AM 62  <i>Article 33 a</i>		
	<i>Adherence to an approved code of conduct as pursuant to Article 42 of Regulation (EU) 2016/679 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 and 2.</i>		deletion
<i>Article 34</i>	AM 63  <i>Article 34</i>	<i>Article 34</i>	
<b>Confidentiality of electronic communications</b>	<del><b>Confidentiality of electronic communications</b></del>	<i>Confidentiality of electronic communications data</i>	New Chapter on confidentiality. See below Article 38a
Union institutions and bodies shall ensure the confidentiality of electronic communications, in particular by securing their	<del>Union institutions and bodies shall ensure the confidentiality of electronic communications, in particular by securing their electronic communication networks</del>	Union institutions and bodies shall ensure the confidentiality of electronic communications <b>data</b> , in particular by securing their electronic communications	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
electronic communication networks.	<del>in accordance with Regulation (EU) 2017/XXXX.</del>	networks.	
	<i>Article 35 Protection of information related to end-users' terminal equipment</i> <i>moved from Section 2 to Section 2a</i>		
<i>Article 36</i>	AM 64  <del><i>Article 36</i></del>	<i>Article 36</i>	
<i>Directories of users</i>	<i>Directories of users</i>	<i>Directories of users</i>	
1.  Personal data contained in directories of users and access to such directories shall be limited to what is strictly necessary for the specific purposes of the directory.	<del>1.  Personal data contained in directories of users and access to such directories shall be limited to what is strictly necessary for the specific purposes of the directory.</del>	1.  Personal data contained in directories of users and access to such directories shall be limited to what is strictly necessary for the specific purposes of the directory.	New Chapter on confidentiality. See below Article 38b
2.  Union institutions and bodies shall take all the necessary measures to prevent personal data contained in those directories, regardless of whether they are accessible to the public or not, from being used for	<del>2.  Union institutions and bodies shall take all the necessary measures to prevent personal data contained in those directories, regardless of whether they are accessible to the public or not, from being used for</del>	2.  Union institutions and bodies shall take all the necessary measures to prevent personal data contained in those directories, regardless of whether they are accessible to the public or not, from being used for	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
direct marketing purposes.	<del>direct marketing purposes.</del>	direct marketing purposes.	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<i>Article 37</i>	<i>Article 37</i>	<i>Article 37</i>	
<b><i>Notification of a personal data breach to the European Data Protection Supervisor</i></b>	<b><i>Notification of a personal data breach to the European Data Protection Supervisor</i></b>	<b><i>Notification of a personal data breach to the European Data Protection Supervisor</i></b>	
<p>1.</p> <p>In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the European Data Protection Supervisor, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the European Data Protection Supervisor is not made within 72 hours, it shall be accompanied by reasons for the delay.</p>	<p>1.</p> <p>In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the European Data Protection Supervisor, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the European Data Protection Supervisor is not made within 72 hours, it shall be accompanied by reasons for the delay.</p>	<p>1.</p> <p>In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the European Data Protection Supervisor, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the European Data Protection Supervisor is not made within 72 hours, it shall be accompanied by reasons for the delay.</p>	
<p>2.</p> <p>The processor shall notify the controller without undue delay after becoming aware of a personal data</p>	<p>2.</p> <p>The processor shall notify the controller without undue delay after becoming aware of a personal data</p>	<p>2.</p> <p>The processor shall notify the controller without undue delay after becoming aware of a personal</p>	



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
breach.	breach.	data breach.	
3.  The notification referred to in paragraph 1 shall at least:	3.  The notification referred to in paragraph 1 shall at least:	3.  The notification referred to in paragraph 1 shall at least:	
(a)  describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;	(a)  describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;	(a)  describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;	
(b)  communicate the name and contact details of the data protection officer;	(b)  communicate the name and contact details of the data protection officer;	(b)  communicate the name and contact details of the data protection officer;	
(c)  describe the likely consequences of the personal data breach;	(c)  describe the likely consequences of the personal data breach;	(c)  describe the likely consequences of the personal data breach;	
(d)	(d)	(d)	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.	describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.	describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.	
4.  Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.	4.  Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.	4.  Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.	
5.  The controller shall inform the data protection officer about the personal data breach.	5.  The controller shall inform the data protection officer about the personal data breach.	5.  The controller shall inform the data protection officer about the personal data breach.	
6.  The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the	6.  The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the	6.  The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
European Data Protection Supervisor to verify compliance with this Article.	European Data Protection Supervisor to verify compliance with this Article.	European Data Protection Supervisor to verify compliance with this Article.	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<i>Article 38</i>	<i>Article 38</i>	<i>Article 38</i>	
<b><i>Communication of a personal data breach to the data subject</i></b>	<b><i>Communication of a personal data breach to the data subject</i></b>	<b><i>Communication of a personal data breach to the data subject</i></b>	
1.  When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.	1.  When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.	1.  When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.	
2.  The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 37(3).	2.  The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 37(3).	2.  The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 37(3).	
3.  The communication to the data subject referred to in paragraph 1	3.  The communication to the data subject referred to in paragraph 1	3.  The communication to the data subject referred to in paragraph 1	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
shall not be required if any of the following conditions are met:	shall not be required if any of the following conditions are met:	shall not be required if any of the following conditions are met:	
(a)  the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;	(a)  the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;	(a)  the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;	
(b)  the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;	(b)  the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;	(b)  the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;	
(c)  it would involve disproportionate effort. In such a case, there shall instead be a public communication	(c)  it would involve disproportionate effort. In such a case, there shall instead be a public communication	(c)  it would involve disproportionate effort. In such a case, there shall instead be a public communication	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
or similar measure whereby the data subjects are informed in an equally effective manner.	or similar measure whereby the data subjects are informed in an equally effective manner.	or similar measure whereby the data subjects are informed in an equally effective manner.	
4.  If the controller has not already communicated the personal data breach to the data subject, the European Data Protection Supervisor, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.	4.  If the controller has not already communicated the personal data breach to the data subject, the European Data Protection Supervisor, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.	4.  If the controller has not already communicated the personal data breach to the data subject, the European Data Protection Supervisor, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.	
	<b>AM 65</b>  <b><i>SECTION 2a</i></b>  <b><i>CONFIDENTIALITY OF ELECTRONIC COMMUNICATIONS</i></b>		<b><i>SECTION 2a</i></b>  <b><i>CONFIDENTIALITY OF ELECTRONIC COMMUNICATIONS</i></b>
	<b>AM 66</b>  <b><i>Article 38a</i></b>		<b><i>Article 38a</i></b>
	<b><i>Confidentiality of electronic</i></b>		<b><i>Confidentiality of electronic</i></b>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>communications</i>		<i>communications</i>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>Union institutions and bodies shall ensure the confidentiality of electronic communications, in particular by securing their electronic communication networks.</i>		Union institutions and bodies shall ensure the confidentiality of electronic communications, in particular by securing their electronic communication networks.
<i>Article 35</i>	<i>Article 35</i> <b>Moved down to Section 2a (new) from Section 2</b>	<i>Article 35</i>	<i>Article 38aa</i>
<i>Protection of information related to end-users' terminal equipment</i>	<i>Protection of information related to end-users' terminal equipment</i>	<i>Protection of information stored in and related to end-users' terminal equipment</i>	Protection of information transmitted to, stored in, related to, processed by and collected from users' terminal equipment
Union institutions and bodies shall protect the information related to end-users' terminal equipment accessing their publicly available websites and mobile applications in accordance with Regulation (EU) XX/XXXX [new ePrivacy Regulation], in particular Article 8 thereof.	Union institutions and bodies shall protect the information related to end-users' terminal equipment accessing their publicly available websites and mobile applications in accordance with Regulation (EU) XX/XXXX [new ePrivacy Regulation], in particular Article 8 thereof.	Union institutions and bodies shall protect the information <b>stored in and</b> related to end-users' terminal equipment accessing their publicly available websites and mobile applications in accordance with Regulation (EU) XX/XXXX [new ePrivacy Regulation], in particular Article 8 thereof.	Union institutions and bodies shall protect the information transmitted to, stored in, related to, processed by and collected from users' terminal equipment accessing their publicly available websites and mobile applications in accordance with Article 5(3) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
	AM 67 <i>Article 38b</i>		<i>Article 38b</i>
	<i>Directories of users</i>		<i>Directories of users</i>
	1. <i>Personal data contained in directories of users and access to such directories shall be limited to what is strictly necessary for the specific purposes of the directory.</i>		1. Personal data contained in directories of users and access to such directories shall be limited to what is strictly necessary for the specific purposes of the directory.
	2. <i>Union institutions and bodies shall take all the necessary measures to prevent personal data contained in those directories from being used for direct marketing purposes, regardless of whether they are accessible to the public or not.</i>		2. Union institutions and bodies shall take all the necessary measures to prevent personal data contained in those directories from being used for direct marketing purposes regardless of whether they are accessible to the public or not.

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<b>SECTION 3</b> <b>DATA PROTECTION</b> <b>IMPACT</b> <b>ASSESSMENT AND</b> <b>PRIOR</b> <b>CONSULTATION</b>	<b>SECTION 3</b> <b>DATA PROTECTION</b> <b>IMPACT ASSESSMENT</b> <b>AND PRIOR</b> <b>CONSULTATION</b>	<b>SECTION 3</b> <b>DATA PROTECTION</b> <b>IMPACT</b> <b>ASSESSMENT AND</b> <b>PRIOR</b> <b>CONSULTATION</b>	
<i>Article 39</i>	<i>Article 39</i>	<i>Article 39</i>	
<i>Data protection impact assessment</i>	<i>Data protection impact assessment</i>	<i>Data protection impact assessment</i>	
1.  Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.	1.  Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.	1.  Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
		similar high risks.	
2.  The controller shall seek the advice of the data protection officer when carrying out a data protection impact assessment.	2.  The controller shall seek the advice of the data protection officer when carrying out a data protection impact assessment.	2.  The controller shall seek the advice of the data protection officer when carrying out a data protection impact assessment.	
3.  A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:	3.  A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:	3.  A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:	
(a)  a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;	(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;	(a)  a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;	
(b)	(b)	(b)	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
processing on a large scale of special categories of data referred to in Article 10, or of personal data relating to criminal convictions and offences referred to in Article 11; or	processing on a large scale of special categories of data referred to in Article 10, or of personal data relating to criminal convictions and offences referred to in Article 11; or	processing on a large scale of special categories of data referred to in Article 10, or of personal data relating to criminal convictions and offences referred to in Article 11; or	
(c) a systematic monitoring of a publicly accessible area on a large scale.	(c) a systematic monitoring of a publicly accessible area on a large scale.	(c) a systematic monitoring of a publicly accessible area on a large scale.	
4. The European Data Protection Supervisor shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1.	4. The European Data Protection Supervisor shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1.	4. The European Data Protection Supervisor shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1.	
5. The European Data Protection Supervisor may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is	5. The European Data Protection Supervisor may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is	5. The European Data Protection Supervisor may also establish and make public a list of the kind of processing operations for which no data protection impact assessment	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
required.	required.	is required.	
		<b>5a.</b>  <b>Prior to the adoption of the lists referred to in paragraphs 4 and 5, the European Data Protection Supervisor shall request the European Data Protection Board to examine such lists in accordance with Article 70(1)(e) of Regulation (EU) 2016/679, where such lists may affect the free movement of personal data within the Union, in particular where they refer to processing operations by a controller acting jointly with one or more controllers other than Union institutions and bodies.</b>	5a. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the European Data Protection Supervisor shall request the European Data Protection Board to examine such lists in accordance with Article 70(1)(e) of Regulation (EU) 2016/679 where they refer to processing operations by a controller acting jointly with one or more controllers other than Union institutions and bodies.
6.  The assessment shall contain at least:	6.  The assessment shall contain at least:	6.  The assessment shall contain at least:	
(a)  a systematic description of the envisaged processing operations and	(a)  systematic description of the envisaged processing operations and the purposes of the processing;	(a)  a systematic description of the envisaged processing operations	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
the purposes of the processing;		and the purposes of the processing;	
(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;	(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;	(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;	
(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and	(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and	(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and	
(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.	(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.	(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.	
7.	7.	7.	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
Compliance with approved codes of conduct referred to in Article 40 of the Regulation (EU) 2016/679 by the relevant processors other than Union institutions and bodies shall be taken into due account in assessing the impact of the processing operations performed by such processors, in particular for the purposes of a data protection impact assessment.	Compliance with approved codes of conduct referred to in Article 40 of the Regulation (EU) 2016/679 by the relevant processors other than Union institutions and bodies shall be taken into due account in assessing the impact of the processing operations performed by such processors, in particular for the purposes of a data protection impact assessment.	Compliance with approved codes of conduct referred to in Article 40 of the Regulation (EU) 2016/679 by the relevant processors other than Union institutions and bodies shall be taken into due account in assessing the impact of the processing operations performed by such processors, in particular for the purposes of a data protection impact assessment.	
8.  Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of public interests or the security of processing operations.	8.  Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of public interests or the security of processing operations.	8.  Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of public interests or the security of processing operations.	
9.  Where processing pursuant to point (a) or (b) of Article 5(1) has a legal basis in a legal act adopted on the basis of the Treaties, which regulates the specific processing operation or set of operations in	9.  Where processing pursuant to point (a) or (b) of Article 5(1) has a legal basis in a legal act adopted on the basis of the Treaties, which regulates the specific processing operation or set of operations in	9.  Where processing pursuant to point (a) or (b) of Article 5(1) has a legal basis in a legal act adopted on the basis of the Treaties, which regulates the specific processing operation or set of operations in	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
question, and where a data protection impact assessment has already been carried out as part of a general impact assessment preceding the adoption of that legal act, paragraphs 1 to 6 shall not apply unless the Union law provides otherwise.	question, and where a data protection impact assessment has already been carried out as part of a general impact assessment preceding the adoption of that legal act, paragraphs 1 to 6 shall not apply unless the Union law provides otherwise.	question, and where a data protection impact assessment has already been carried out as part of a general impact assessment preceding the adoption of that legal act, paragraphs 1 to 6 shall not apply unless the Union law provides otherwise.	
10.  Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.	10.  Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.	10.  Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.	
<i>Article 40</i>	<i>Article 40</i>	<i>Article 40</i>	
<i>Prior consultation</i>	<i>Prior consultation</i>	<i>Prior consultation</i>	
1.  The controller shall consult the European Data Protection Supervisor prior to processing where a data protection impact	1.  The controller shall consult the European Data Protection Supervisor prior to processing where a data protection impact	1.  The controller shall consult the European Data Protection Supervisor prior to processing where a data protection impact	



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
assessment under Article 39 indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means	assessment under Article 39 indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means	assessment under Article 39 indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
in terms of available technologies and costs of implementation. The controller shall seek the advice of the data protection officer about the need for prior consultation.	in terms of available technologies and costs of implementation. The controller shall seek the advice of the data protection officer about the need for prior consultation.	in terms of available technologies and costs of implementation. The controller shall seek the advice of the data protection officer about the need for prior consultation.	
<p>2.</p> <p>Where the European Data Protection Supervisor is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the European Data Protection Supervisor shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 59. That period may be extended by six weeks, taking into account the complexity of the intended processing. The European</p>	<p>2.</p> <p>Where the European Data Protection Supervisor is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the European Data Protection Supervisor shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 59. That period may be extended by six weeks, taking into account the complexity of the intended processing. The European</p>	<p>2.</p> <p>Where the European Data Protection Supervisor is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the European Data Protection Supervisor shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 59. That period may be extended by six weeks, taking into account the complexity of the intended processing. The European</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
Data Protection Supervisor shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the European Data Protection Supervisor has obtained information it has requested for the purposes of the consultation.	Data Protection Supervisor shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the European Data Protection Supervisor has obtained information it has requested for the purposes of the consultation.	Data Protection Supervisor shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the European Data Protection Supervisor has obtained information it has requested for the purposes of the consultation.	
3.  When consulting the European Data Protection Supervisor pursuant to paragraph 1, the controller shall provide the European Data Protection Supervisor with:	3.  When consulting the European Data Protection Supervisor pursuant to paragraph 1, the controller shall provide the European Data Protection Supervisor with:	3.  When consulting the European Data Protection Supervisor pursuant to paragraph 1, the controller shall provide the European Data Protection Supervisor with:	
(a)  where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing;	(a)  where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing;	(a)  where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing;	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
(b) the purposes and means of the intended processing;	(b) the purposes and means of the intended processing;	(b) the purposes and means of the intended processing;	
(c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;	(c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;	(c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;	
(d) the contact details of the data protection officer;	(d) the contact details of the data protection officer;	(d) the contact details of the data protection officer;	
(e) the data protection impact assessment provided for in Article 39; and	(e) the data protection impact assessment provided for in Article 39; and	(e) the data protection impact assessment provided for in Article 39; and	
(f) any other information requested by the European Data Protection Supervisor.	(f) any other information requested by the European Data Protection Supervisor. <sup>a</sup>	(f) any other information requested by the European Data Protection Supervisor.	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>4.</p> <p>The Commission may, by means of implementing act, determine a list of cases in which the controllers shall consult with, and obtain prior authorisation from, the European Data Protection Supervisor in relation to processing for the performance of a task carried out by the controller in the public interest, including the processing of such data in relation to social protection and public health.</p>	<p>4.</p> <p>The Commission may, by means of implementing act, determine a list of cases in which the controllers shall consult with, and obtain prior authorisation from, the European Data Protection Supervisor in relation to processing for the performance of a task carried out by the controller in the public interest, including the processing of such data in relation to social protection and public health.</p>	<p>4.</p> <p>The Commission may, by means of implementing act, determine a list of cases in which the controllers shall consult with, and obtain prior authorisation from, the European Data Protection Supervisor in relation to processing for the performance of a task carried out by the controller in the public interest, including the processing of such data in relation to social protection and public health.</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<b>SECTION 4</b> <b>INFORMATION AND LEGISLATIVE CONSULTATION</b>	<b>SECTION 4</b> <b>INFORMATION AND LEGISLATIVE CONSULTATION</b>	<b>SECTION 4</b> <b>INFORMATION AND LEGISLATIVE CONSULTATION</b>	
<i>Article 41</i>	<i>Article 41</i>	<i>Article 41</i>	
<i>Information</i>	<i>Information</i>	<i>Information and consultation</i>	
The Union institutions and bodies shall inform the European Data Protection Supervisor when drawing up administrative measures and internal rules relating to the processing of personal data involving a Union institution or body alone or jointly with others.	<b>AM 68</b> The Union institutions and bodies shall inform the European Data Protection Supervisor when drawing up administrative measures <del>and internal rules</del> relating to the processing of personal data involving a Union institution or body alone or jointly with others.	<b>1.</b> The Union institutions and bodies shall inform the European Data Protection Supervisor when drawing up administrative measures <b>and internal rules</b> relating to the processing of personal data involving a Union institution or body alone or jointly with others.	
		<b>2.</b> <b>The Union institutions and bodies shall consult the European Data Protection Supervisor when drawing up the internal rules referred to in</b>	Council suggestion:  2. The Union institutions and bodies

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
		Article 25(5).	shall consult the European Data Protection Supervisor when drawing up the internal rules referred to in Article 25(5).

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<i>Article 42</i>	<i>Article 42</i>	<i>Article 42</i>	
<i>Legislative consultation</i>	<i>Legislative consultation</i>	<i>Legislative consultation</i>	
<p>1.</p> <p>Following the adoption of proposals for a legislative act and of recommendations or proposals to the Council pursuant to Article 218 TFEU and when preparing delegated acts or implementing acts, which have an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data, the Commission shall consult the European Data Protection Supervisor.</p>	<p><b>AM 69</b></p> <p>1.</p> <p><del>Following the adoption of</del> <b>When adopting</b> proposals for a legislative act and of recommendations or proposals to the Council pursuant to Article 218 TFEU and when preparing delegated acts or implementing acts, <del>which have an impact on</del> <b>relating to</b> the protection of <del>individuals'</del> <b>natural persons'</b> rights and freedoms with regard to the processing of personal data, the Commission shall consult the European Data Protection Supervisor.</p>	<p>1.</p> <p>Following the adoption of proposals for a legislative act and of recommendations or proposals to the Council pursuant to Article 218 TFEU and when preparing delegated acts or implementing acts, which have an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data, the Commission shall consult the European Data Protection Supervisor.</p>	<p>Council suggestion:</p> <p>1. Following the adoption of proposals for a legislative act and of recommendations or proposals to the Council pursuant to Article 218 TFEU and when preparing delegated acts or implementing acts, which have an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data, the Commission shall consult the European Data Protection Supervisor.</p>
<p>2.</p> <p>Where an act referred to in paragraph 1 is of particular importance for the protection of individuals' rights and freedoms with regard to the processing of personal data, the Commission may</p>	<p>2.</p> <p>Where an act referred to in paragraph 1 is of particular importance for the protection of individuals' rights and freedoms with regard to the processing of personal data, the Commission may</p>	<p>2.</p> <p>Where an act referred to in paragraph 1 is of particular importance for the protection of individuals' rights and freedoms with regard to the processing of personal data, the Commission</p>	



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
also consult the European Data Protection Board. In such cases the European Data Protection Supervisor and the European Data Protection Board shall coordinate their work with a view to issue a joint opinion.	also consult the European Data Protection Board. In such cases the European Data Protection Supervisor and the European Data Protection Board shall coordinate their work with a view to issue a joint opinion.	may also consult the European Data Protection Board. In such cases the European Data Protection Supervisor and the European Data Protection Board shall coordinate their work with a view to issue a joint opinion.	
3.  The advice referred to in paragraphs 1 and 2 shall be provided in writing within a period of up to eight weeks of receipt of the request for consultation referred to in paragraphs 1 and 2. In urgent cases, or otherwise appropriate, the Commission may shorten the deadline.	3.  The advice referred to in paragraphs 1 and 2 shall be provided in writing within a period of up to eight weeks of receipt of the request for consultation referred to in paragraphs 1 and 2. In urgent cases, or otherwise appropriate, the Commission may shorten the deadline.	3.  The advice referred to in paragraphs 1 and 2 shall be provided in writing within a period of up to eight weeks of receipt of the request for consultation referred to in paragraphs 1 and 2. In urgent cases, or otherwise appropriate, the Commission may shorten the deadline.	
4.  This Article shall not apply where the Commission is required, pursuant to Regulation (EU) 2016/679, to consult the European Data Protection Board.	4.  This Article shall not apply where the Commission is required, pursuant to Regulation (EU) 2016/679, to consult the European Data Protection Board.	4.  This Article shall not apply where the Commission is required, pursuant to Regulation (EU) 2016/679, to consult the European Data Protection Board.	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<b>SECTION 5</b> <b>OBLIGATION TO REACT TO ALLEGATIONS</b>	<b>SECTION 5</b> <b>OBLIGATION TO REACT TO ALLEGATIONS</b>	<b>SECTION 5</b> <b>OBLIGATION TO REACT TO ALLEGATIONS</b>	
<i>Article 43</i>	<i>Article 43</i>	<i>Article 43</i>	
<i>Obligation to react to allegations</i>	<i>Obligation to react to allegations</i>	<i>Obligation to react to allegations</i>	
Where the European Data Protection Supervisor exercises the powers provided for in points (a), (b) and (c) of Article 59(2), the controller or processor concerned shall inform the European Data Protection Supervisor of its views within a reasonable period to be specified by the European Data Protection Supervisor, taking into account the circumstances of each case. The reply shall also include a description of the measures taken, if any, in response to the remarks of the European Data Protection Supervisor.	Where the European Data Protection Supervisor exercises the powers provided for in points (a), (b) and (c) of Article 59(2), the controller or processor concerned shall inform the European Data Protection Supervisor of its views within a reasonable period to be specified by the European Data Protection Supervisor, taking into account the circumstances of each case. The reply shall also include a description of the measures taken, if any, in response to the remarks of the European Data Protection Supervisor.	Where the European Data Protection Supervisor exercises the powers provided for in points (a), (b) and (c) of Article 59(2), the controller or processor concerned shall inform the European Data Protection Supervisor of its views within a reasonable period to be specified by the European Data Protection Supervisor, taking into account the circumstances of each case. The reply shall also include a description of the measures taken, if any, in response to the remarks of the European Data Protection Supervisor.	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<b>SECTION 6</b> <b>DATA PROTECTION OFFICER</b>	<b>SECTION 6</b> <b>DATA PROTECTION OFFICER</b>	<b>SECTION 6</b> <b>DATA PROTECTION OFFICER</b>	
<i>Article 44</i>	<i>Article 44</i>	<i>Article 44</i>	
<i>Designation of the data protection officer</i>	<i>Designation of the data protection officer</i>	<i>Designation of the data protection officer</i>	
1.  Each Union institution or body shall designate a data protection officer.	1.  Each Union institution or body shall designate a data protection officer.	1.  Each Union institution or body shall designate a data protection officer.	
2.  Union institutions and bodies may designate a single data protection officer for several of them, taking into account their organisational structure and size.	2.  Union institutions and bodies may designate a single data protection officer for several of them, taking into account their organisational structure and size.	2.  Union institutions and bodies may designate a single data protection officer for several of them, taking into account their organisational structure and size.	
3.  The data protection officer shall be designated on the basis of professional qualities and, in	3.  The data protection officer shall be designated on the basis of professional qualities and, in	3.  The data protection officer shall be designated on the basis of professional qualities and, in	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 46.	particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 46.	particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 46.	
<p>4.</p> <p>The data protection officer may be a staff member of the Union institution or body, or fulfil the tasks on the basis of a service contract.</p>	<p><b>AM 70</b></p> <p>4.</p> <p>The data protection officer <del>may</del> <b>shall</b> be a staff member of the Union institution or body, <del>or fulfil the</del> <b><i>In exceptional circumstances, taking into account their size and if the conditions set out in paragraph 2 are not met, Union institutions and bodies may designate a data protection officer who fulfils his or her</i></b> tasks on the basis of a service contract.</p>	<p>4.</p> <p>The data protection officer may be a staff member of the Union institution or body, or fulfil the tasks on the basis of a service contract.</p>	<p>Council suggestion:</p> <p>4. The data protection officer shall be a staff member of the Union institution or body. Taking into account their size and if the conditions set out in paragraph 2 are not met, Union institutions and bodies may designate a data protection officer who fulfils his or her tasks on the basis of a service contract.</p>
<p>5.</p> <p>The Union institutions and bodies shall publish the contact details of the data protection officer and communicate them to the European Data Protection Supervisor.</p>	<p>5.</p> <p>The Union institutions and bodies shall publish the contact details of the data protection officer and communicate them to the European Data Protection Supervisor.</p>	<p>5.</p> <p>The Union institutions and bodies shall publish the contact details of the data protection officer and communicate them to the European Data Protection Supervisor.</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<i>Article 45</i>	<i>Article 45</i>	<i>Article 45</i>	
<i>Position of the data protection officer</i>	<i>Position of the data protection officer</i>	<i>Position of the data protection officer</i>	
1.  The Union institutions and bodies shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.	1.  The Union institutions and bodies shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.	1.  The Union institutions and bodies shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.	
2.  The Union institutions and bodies shall support the data protection officer in performing the tasks referred to in Article 46 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.	2.  The Union institutions and bodies shall support the data protection officer in performing the tasks referred to in Article 46 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.	2.  The Union institutions and bodies shall support the data protection officer in performing the tasks referred to in Article 46 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.	
3.  The Union institutions and bodies shall ensure that the data protection	3.  The Union institutions and bodies shall ensure that the data protection	3.  The Union institutions and bodies shall ensure that the data protection	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
officer does not receive any instructions regarding the exercise of his or her tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his or her tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.	officer does not receive any instructions regarding the exercise of his or her tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his or her tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.	officer does not receive any instructions regarding the exercise of his or her tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his or her tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.	
4.  Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.	4.  Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.	4.  Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.	
5.  The data protection officer and his or her staff shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union law.	<b>AM 71</b>  5.  The data protection officer <del>and his or her staff</del> shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union law.	5.  The data protection officer and his or her staff shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union law.	5. The data protection officer and his or her staff shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union law

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>6.</p> <p>The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.</p>	<p>6.</p> <p>The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.</p>	<p>6.</p> <p>The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.</p>	
<p>7.</p> <p>The data protection officer may be consulted by the controller and the processor, by the Staff Committee concerned and by any individual, without going through the official channels, on any matter concerning the interpretation or application of this Regulation. No one shall suffer prejudice on account of a matter brought to the attention of the competent data protection officer alleging that a breach of the provisions of this Regulation has taken place.</p>	<p>7.</p> <p>The data protection officer may be consulted by the controller and the processor, by the Staff Committee concerned and by any individual, without going through the official channels, on any matter concerning the interpretation or application of this Regulation. No one shall suffer prejudice on account of a matter brought to the attention of the competent data protection officer alleging that a breach of the provisions of this Regulation has taken place.</p>	<p>7.</p> <p>The data protection officer may be consulted by the controller and the processor, by the Staff Committee concerned and by any individual, without going through the official channels, on any matter concerning the interpretation or application of this Regulation. No one shall suffer prejudice on account of a matter brought to the attention of the competent data protection officer alleging that a breach of the provisions of this Regulation has taken place.</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>8.</p> <p>The data protection officer shall be designated for a term of three to five years and shall be eligible for reappointment. The data protection officer may be dismissed from the post by the Union institution or body which designated him or her only with the consent of the European Data Protection Supervisor, if he or she no longer fulfils the conditions required for the performance of his or her duties.</p>	<p>8.</p> <p>The data protection officer shall be designated for a term of three to five years and shall be eligible for reappointment. The data protection officer may be dismissed from the post by the Union institution or body which designated him or her only with the consent of the European Data Protection Supervisor, if he or she no longer fulfils the conditions required for the performance of his or her duties.</p>	<p>8.</p> <p>The data protection officer shall be designated for a term of three to five years and shall be eligible for reappointment. The data protection officer may be dismissed from the post by the Union institution or body which designated him or her only with the consent of the European Data Protection Supervisor, if he or she no longer fulfils the conditions required for the performance of his or her duties.</p>	
<p>9.</p> <p>After his or her designation the data protection officer shall be registered with the European Data Protection Supervisor by the Union institution or body which designated him or her.</p>	<p>9.</p> <p>After his or her designation the data protection officer shall be registered with the European Data Protection Supervisor by the Union institution or body which designated him or her.</p>	<p>9.</p> <p>After his or her designation the data protection officer shall be registered with the European Data Protection Supervisor by the Union institution or body which designated him or her.</p>	



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<i>Article 46</i>	<i>Article 46</i>	<i>Article 46</i>	
<b><i>Tasks of the data protection officer</i></b>	<b><i>Tasks of the data protection officer</i></b>	<b><i>Tasks of the data protection officer</i></b>	
1.  The data protection officer shall have the following tasks:	1.  The data protection officer shall have the following tasks:	1.  The data protection officer shall have the following tasks:	
(a)  inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union data protection provisions;	(a)  inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union data protection provisions;	(a)  inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union data protection provisions;	
(b)  ensure in an independent manner the internal application of this Regulation and to monitor compliance with this Regulation, with other applicable Union law containing data protection provisions and with the policies of the controller or processor in relation to the protection of personal	(b)  ensure in an independent manner the internal application of this Regulation and to monitor compliance with this Regulation, with other applicable Union law containing data protection provisions and with the policies of the controller or processor in relation to the protection of personal	(b)  ensure in an independent manner the internal application of this Regulation and to monitor compliance with this Regulation, with other applicable Union law containing data protection provisions and with the policies of the controller or processor in relation to the protection of	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
data, including the assignment of responsibilities, the raising of awareness and training of staff involved in processing operations, and the related audits;	data, including the assignment of responsibilities, the raising of awareness and training of staff involved in processing operations, and the related audits;	personal data, including the assignment of responsibilities, the raising of awareness and training of staff involved in processing operations, and the related audits;	
(c) ensure that data subjects are informed of their rights and obligations pursuant to this Regulation;	(c) ensure that data subjects are informed of their rights and obligations pursuant to this Regulation;	(c) ensure that data subjects are informed of their rights and obligations pursuant to this Regulation;	
(d) provide advice where requested as regards the necessity for a notification or a communication of personal data breach pursuant to Articles 37 and 38;	(d) provide advice where requested as regards the necessity for a notification or a communication of personal data breach pursuant to Articles 37 and 38;	(d) provide advice where requested as regards the necessity for a notification or a communication of personal data breach pursuant to Articles 37 and 38;	
(e) provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 39 and to consult the European Data Protection Supervisor in case of doubt as to the need for a data	(e) provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 39 and to consult the European Data Protection Supervisor in case of doubt as to the need for a data	(e) provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 39 and to consult the European Data Protection Supervisor in case of doubt as to the need for a data	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
protection impact assessment;	protection impact assessment;	protection impact assessment;	
(f)  provide advice where requested as regards the need for prior consultation of the European Data Protection Supervisor pursuant to Article 40 and to consult the European Data Protection Supervisor in case of doubt as to the need for a prior consultation;	(f)  provide advice where requested as regards the need for prior consultation of the European Data Protection Supervisor pursuant to Article 40 and to consult the European Data Protection Supervisor in case of doubt as to the need for a prior consultation;	(f)  provide advice where requested as regards the need for prior consultation of the European Data Protection Supervisor pursuant to Article 40 and to consult the European Data Protection Supervisor in case of doubt as to the need for a prior consultation;	
(g)  respond to requests from the European Data Protection Supervisor and, within the sphere of his or her competence, to cooperate and consult with the European Data Protection Supervisor at the latter's request or on his or her own initiative.	(g)  respond to requests from the European Data Protection Supervisor and, within the sphere of his or her competence, to cooperate and consult with the European Data Protection Supervisor at the latter's request or on his or her own initiative.	(g)  respond to requests from the European Data Protection Supervisor and, within the sphere of his or her competence, to cooperate and consult with the European Data Protection Supervisor at the latter's request or on his or her own initiative.	
	<b>AM 72</b>  <i>(ga)</i>  <i>nsure that the rights and freedoms of data subjects are not adversely</i>		(ga) ensure that the rights and freedoms of data subjects are not adversely affected by processing operations.

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>affected by processing operations.</i>		

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>2.</p> <p>The data protection officer may make recommendations for the practical improvement of data protection to the controller and the processor and advise them on matters concerning the application of data protection provisions. Furthermore he or she may, on his or her own initiative or at the request of the controller or the processor, the Staff Committee concerned or any individual, investigate matters and occurrences directly relating to his or her tasks and which come to his or her notice, and report back to the person who commissioned the investigation or to the controller or the processor.</p>	<p>2.</p> <p>The data protection officer may make recommendations for the practical improvement of data protection to the controller and the processor and advise them on matters concerning the application of data protection provisions. Furthermore he or she may, on his or her own initiative or at the request of the controller or the processor, the Staff Committee concerned or any individual, investigate matters and occurrences directly relating to his or her tasks and which come to his or her notice, and report back to the person who commissioned the investigation or to the controller or the processor.</p>	<p>2.</p> <p>The data protection officer may make recommendations for the practical improvement of data protection to the controller and the processor and advise them on matters concerning the application of data protection provisions. Furthermore he or she may, on his or her own initiative or at the request of the controller or the processor, the Staff Committee concerned or any individual, investigate matters and occurrences directly relating to his or her tasks and which come to his or her notice, and report back to the person who commissioned the investigation or to the controller or the processor.</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
3.  Further implementing rules concerning the data protection officer shall be adopted by each Union institution or body. The implementing rules shall in particular concern the tasks, duties and powers of the data protection officer.	3.  Further implementing rules concerning the data protection officer shall be adopted by each Union institution or body. The implementing rules shall in particular concern the tasks, duties and powers of the data protection officer.	3.  Further implementing rules concerning the data protection officer shall be adopted by each Union institution or body. The implementing rules shall in particular concern the tasks, duties and powers of the data protection officer.	
<b>CHAPTER V</b>  <b>Transfers of personal data to third countries or international organisations</b>	<b>CHAPTER V</b>  <b>Transfers of personal data to third countries or international organisations</b>	<b>CHAPTER V</b>  <b>Transfers of personal data to third countries or international organisations</b>	
<i>Article 47</i>	<i>Article 47</i>	<i>Article 47</i>	
<i>General principle for transfers</i>	<i>General principle for transfers</i>	<i>General principle for transfers</i>	
Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other	Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other	Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to	provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to	other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to	
another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.	another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.	another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.	
<i>Article 48</i>	<i>Article 48</i>	<i>Article 48</i>	
<i>Transfers on the basis of an adequacy decision</i>	<i>Transfers on the basis of an adequacy decision</i>	<i>Transfers on the basis of an adequacy decision</i>	
1.  A transfer of personal data to a third country or international organisation may take place where the Commission has decided pursuant to Article 45(3) of Regulation (EU) 2016/679 that an adequate level of protection is ensured in the third	<b>AM 73</b>  1.  A transfer of personal data to a third country or international organisation may take place where the Commission has decided pursuant to Article 45(3) of Regulation (EU)	1.  A transfer of personal data to a third country or international organisation may take place where the Commission has decided pursuant to Article 45(3) of Regulation (EU) 2016/679 that an adequate level of protection is	1. A transfer of personal data to a third country or international organisation may take place where the Commission has decided pursuant to Article 45(3) of Regulation (EU) 2016/679 or to Article 36 of Directive (EU) 2016/680 that an adequate level of protection is ensured in the third

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
country, a territory or one or more specified sectors within that third country, or within the international organisation and the personal data are transferred solely to allow tasks covered by the competence of the controller to be carried out.	2016/679 <i>or to Article 36 of Directive (EU) 2016/680</i> , that an adequate level of protection is ensured in the third country, a territory or one or more specified sectors within that third country, or within the international organisation and the personal data are transferred solely to allow tasks covered by the competence of the controller to be carried out. <b><i>Such a transfer shall not require any specific authorisation.</i></b>	ensured in the third country, a territory or one or more specified sectors within that third country, or within the international organisation and the personal data are transferred solely to allow tasks covered by the competence of the controller to be carried out.	country, a territory or one or more specified sectors within that third country, or within the international organisation and the personal data are transferred solely to allow tasks covered by the competence of the controller to be carried out
2. The Union institutions and bodies shall inform the Commission and the European Data Protection Supervisor of cases where they consider the third country or international organisation in question does not ensure an adequate level of protection within the meaning of paragraph 1.	2. The Union institutions and bodies shall inform the Commission and the European Data Protection Supervisor of cases where they consider the third country or international organisation in question does not ensure an adequate level of protection within the meaning of paragraph 1.	2. The Union institutions and bodies shall inform the Commission and the European Data Protection Supervisor of cases where they consider the third country or international organisation in question does not ensure an adequate level of protection within the meaning of paragraph 1.	
3. The Union institutions and bodies shall take the necessary measures to comply with decisions taken by the Commission when it establishes, pursuant to Article 45(3) and (5) of	3. The Union institutions and bodies shall take the necessary measures to comply with decisions taken by the Commission when it establishes, pursuant to Article 45(3) and (5) of	3. The Union institutions and bodies shall take the necessary measures to comply with decisions taken by the Commission when it establishes, pursuant to Article	



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
Regulation (EU) 2016/679, that a third country or an international organisation ensures or no longer ensures an adequate level of protection.	Regulation (EU) 2016/679, that a third country or an international organisation ensures or no longer ensures an adequate level of protection.	45(3) and (5) of Regulation (EU) 2016/679, that a third country or an international organisation ensures or no longer ensures an adequate level of protection.	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<i>Article 49</i>	<i>Article 49</i>	<i>Article 49</i>	
<i>Transfers subject to appropriate safeguards</i>	<i>Transfers subject to appropriate safeguards</i>	<i>Transfers subject to appropriate safeguards</i>	
1. In the absence of a decision pursuant to Article 45(3) of Regulation (EU) 2016/679, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.	<b>AM 74</b> 1. In the absence of a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 <i>or to Article 36(3) of Directive (EU) 2016/680, within the respective scope of those legislative acts</i> , a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.	1. In the absence of a decision pursuant to Article 45(3) of Regulation (EU) 2016/679, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.	1. In the absence of a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 or to Article 36(3) of Directive (EU) 2016/680, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.
2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from the European Data Protection Supervisor, by:	2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from the European Data Protection Supervisor, by:	2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from the European Data Protection Supervisor, by:	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
(a) a legally binding and enforceable instrument between public authorities or bodies;	(a) a legally binding and enforceable instrument between public authorities or bodies;	(a) a legally binding and enforceable instrument between public authorities or bodies;	
(b) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 70(2);	(b) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 70(2);	(b) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 70(2);	
(c) standard data protection clauses adopted by the European Data Protection Supervisor and approved by the Commission pursuant to the examination procedure referred to in Article 70(2);	(c) standard data protection clauses adopted by the European Data Protection Supervisor and approved by the Commission pursuant to the examination procedure referred to in Article 70(2);	(c) standard data protection clauses adopted by the European Data Protection Supervisor and approved by the Commission pursuant to the examination procedure referred to in Article 70(2);	
(d) binding corporate rules, codes of conduct and certification mechanism pursuant to points (b), (e) and (f) of Article 46(2) of Regulation (EU) 2016/679, where the processor is not a Union institution or body.	(d) binding corporate rules, codes of conduct and certification mechanism pursuant to points (b), (e) and (f) of Article 46(2) of Regulation (EU) 2016/679, where the processor is not a Union institution or body.	(d) binding corporate rules, codes of conduct and certification mechanism pursuant to points (b), (e) and (f) of Article 46(2) of Regulation (EU) 2016/679, where the processor is not a Union institution or body.	
3. Subject to the authorisation from the European Data Protection Supervisor, the appropriate safeguards referred to in	3. Subject to the authorisation from the European Data Protection Supervisor, the appropriate safeguards referred to in	3. Subject to the authorisation from the European Data Protection Supervisor, the appropriate safeguards referred to in	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
paragraph 1 may also be provided for, in particular, by:	paragraph 1 may also be provided for, in particular, by:	paragraph 1 may also be provided for, in particular, by:	
(a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or	(a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or	(a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or	
(b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.	(b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.	(b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.	
4. The Union institutions and bodies shall inform the European Data Protection Supervisor of categories of cases where this Article has been applied.	4. The Union institutions and bodies shall inform the European Data Protection Supervisor of categories of cases where this Article has been applied.	4. The Union institutions and bodies shall inform the European Data Protection Supervisor of categories of cases where this Article has been applied.	
5. Authorisations by the European Data Protection Supervisor on the basis of Article 9(7) of Regulation (EC) No 45/2001 shall remain valid until amended, replaced or repealed, if necessary, by the European Data Protection Supervisor.	5. Authorisations by the European Data Protection Supervisor on the basis of Article 9(7) of Regulation (EC) No 45/2001 shall remain valid until amended, replaced or repealed, if necessary, by the European Data Protection Supervisor.	5. Authorisations by the European Data Protection Supervisor on the basis of Article 9(7) of Regulation (EC) No 45/2001 shall remain valid until amended, replaced or repealed, if necessary, by the European Data Protection Supervisor.	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<i>Article 50</i>	<i>Article 50</i>	<i>Article 50</i>	
<i>Transfers or disclosures not authorised by Union law</i>	<i>Transfers or disclosures not authorised by Union law</i>	<i>Transfers or disclosures not authorised by Union law</i>	
Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union, without prejudice to other grounds for transfer pursuant to this Chapter.	Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union, without prejudice to other grounds for transfer pursuant to this Chapter.	Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union, without prejudice to other grounds for transfer pursuant to this Chapter.	
<i>Article 51</i>	<i>Article 51</i>	<i>Article 51</i>	
<i>Derogations for specific situations</i>	<i>Derogations for specific situations</i>	<i>Derogations for specific situations</i>	
1. In the absence of a decision pursuant to Article 45(3) of Regulation (EU) 2016/679, or of appropriate safeguards pursuant to Article 49, a transfer or a set of transfers of personal data to a third	<b>AM 75</b> 1. In the absence of a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 <i>or to Article 36(3) of Directive (EU)</i>	1. In the absence of a decision pursuant to Article 45(3) of Regulation (EU) 2016/679, or of appropriate safeguards pursuant to Article 49, a transfer or a set of transfers of personal data to a third	1. In the absence of a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 or to Article 36(3) of Directive (EU) 2016/680, or of appropriate safeguards pursuant to Article 49,

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
country or an international organisation shall take place only on one of the following conditions:	<b>2016/680, within the respective scope of those legislative acts</b> , or of appropriate safeguards pursuant to Article 49, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:	country or an international organisation shall take place only on one of the following conditions:	a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:
(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;	(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;	(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;	
(b)  the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;	(b)  the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;	(b)  the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;	
(c)  the transfer is necessary for the conclusion or performance of a	(c)  the transfer is necessary for the conclusion or performance of a	(c)  the transfer is necessary for the conclusion or performance of a	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
contract concluded in the interest of the data subject between the controller and another natural or legal person;	contract concluded in the interest of the data subject between the controller and another natural or legal person;	contract concluded in the interest of the data subject between the controller and another natural or legal person;	
(d) the transfer is necessary for important reasons of public interest;	(d) the transfer is necessary for important reasons of public interest;	(d) the transfer is necessary for important reasons of public interest;	
(e) the transfer is necessary for the establishment, exercise or defence of legal claims; or	(e) the transfer is necessary for the establishment, exercise or defence of legal claims; or	(e) the transfer is necessary for the establishment, exercise or defence of legal claims; or	
(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or	(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or	(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or	
(g) the transfer is made from a register which, according to Union law, is	(g) the transfer is made from a register which, according to Union law, is	(g) the transfer is made from a register which, according to Union law, is	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union law for consultation are fulfilled in the particular case.	intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union law for consultation are fulfilled in the particular case.	intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union law for consultation are fulfilled in the particular case.	
		<b>1a.</b>  <b>Points (a), (b) and (c) of paragraph 1 shall not apply to activities carried out by Union institutions and bodies in the exercise of their public powers.</b>	1a. Points (a), (b) and (c) of paragraph 1 shall not apply to activities carried out by Union institutions and bodies in the exercise of their public powers.
2.  A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register, unless authorised by Union law. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons	2.  A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register, unless authorised by Union law. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons	2.  A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register, unless authorised by Union law. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of	



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
or if they are to be the recipients.	or if they are to be the recipients.	those persons or if they are to be the recipients.	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
3.  The public interest referred to in point (d) of paragraph 1 shall be recognised in Union law.	3.  The public interest referred to in point (d) of paragraph 1 shall be recognised in Union law.	3.  The public interest referred to in point (d) of paragraph 1 shall be recognised in Union law.	
4.  In the absence of an adequacy decision, Union law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation.	4.  In the absence of an adequacy decision, Union law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation.	4.  In the absence of an adequacy decision, Union law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation.	
5.  The Union institutions and bodies shall inform the European Data Protection Supervisor of categories of cases where this Article has been applied.	5.  The Union institutions and bodies shall inform the European Data Protection Supervisor of categories of cases where this Article has been applied.	5.  The Union institutions and bodies shall inform the European Data Protection Supervisor of categories of cases where this Article has been applied.	
<i>Article 52</i>	<i>Article 52</i>	<i>Article 52</i>	
<i>International cooperation for the protection of personal data</i>	<i>International cooperation for the protection of personal data</i>	<i>International cooperation for the protection of personal data</i>	
In relation to third countries and	In relation to third countries and	In relation to third countries and	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
international organisations, the European Data Protection Supervisor, in cooperation with the Commission and the European Data Protection Board, shall take appropriate steps to:	international organisations, the European Data Protection Supervisor, in cooperation with the Commission and the European Data Protection Board, shall take appropriate steps to:	international organisations, the European Data Protection Supervisor, in cooperation with the Commission and the European Data Protection Board, shall take appropriate steps to:	
(a)  develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;	(a)  develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;	(a)  develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;	
(b)  provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;	(b)  provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;	(b)  provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;	
(c)	(c)  e	(c)	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;	engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;	engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;	
(d)  promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.	(d)  promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.	(d)  promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.	
<b>CHAPTER VI</b>  <b>THE EUROPEAN DATA PROTECTION SUPERVISOR</b>	<b>CHAPTER VI</b>  <b>THE EUROPEAN DATA PROTECTION SUPERVISOR</b>	<b>CHAPTER VI</b>  <b>THE EUROPEAN DATA PROTECTION SUPERVISOR</b>	
<i>Article 53</i>	<i>Article 53</i>	<i>Article 53</i>	
<i>European Data Protection Supervisor</i>	<i>European Data Protection Supervisor</i>	<i>European Data Protection Supervisor</i>	
1.  The European Data Protection	1.  The European Data Protection	1.  The European Data Protection	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
Supervisor is hereby established.	Supervisor is hereby established.	Supervisor is hereby established.	
<p>2.</p> <p>With respect to the processing of personal data, the European Data Protection Supervisor shall be responsible for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to data protection, is respected by the Union institutions and bodies.</p>	<p>2.</p> <p>With respect to the processing of personal data, the European Data Protection Supervisor shall be responsible for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to data protection, is respected by the Union institutions and bodies.</p>	<p>2.</p> <p>With respect to the processing of personal data, the European Data Protection Supervisor shall be responsible for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to data protection, is respected by the Union institutions and bodies.</p>	
<p>3.</p> <p>The European Data Protection Supervisor shall be responsible for monitoring and ensuring the application of the provisions of this Regulation and any other Union act relating to the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data by a Union institution or body, and for advising Union institutions and bodies and data subjects on all matters concerning the processing of personal data. To those ends the</p>	<p>3.</p> <p>The European Data Protection Supervisor shall be responsible for monitoring and ensuring the application of the provisions of this Regulation and any other Union act relating to the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data by a Union institution or body, and for advising Union institutions and bodies and data subjects on all matters concerning the processing of personal data. To those ends the</p>	<p>3.</p> <p>The European Data Protection Supervisor shall be responsible for monitoring and ensuring the application of the provisions of this Regulation and any other Union act relating to the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data by a Union institution or body, and for advising Union institutions and bodies and data subjects on all matters concerning the processing of personal data. To those ends the</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
European Data Protection Supervisor shall fulfil the tasks provided for in Article 58 and exercise the powers granted in Article 59.	European Data Protection Supervisor shall fulfil the tasks provided for in Article 58 and exercise the powers granted in Article 59.	European Data Protection Supervisor shall fulfil the tasks provided for in Article 58 and exercise the powers granted in Article 59.	
		<b>3a.</b> <b>Regulation (EC) No 1049/2001 shall apply to documents held by the European Data Protection Supervisor. The European Data Protection Supervisor shall adopt detailed rules for applying Regulation (EC) No 1049/2001 with regard to those documents.</b>	3a. Regulation (EC) No 1049/2001 shall apply to documents held by the European Data Protection Supervisor. The European Data Protection Supervisor shall adopt detailed rules for applying Regulation (EC) No 1049/2001 with regard to those documents.
<i>Article 54</i>	<i>Article 54</i>	<i>Article 54</i>	
<i>Appointment of the European Data Protection Supervisor</i>	<i>Appointment of the European Data Protection Supervisor</i>	<i>Appointment of the European Data Protection Supervisor</i>	
1.  The European Parliament and the Council shall appoint the European Data Protection Supervisor by common accord for a term of five years, on the basis of a list drawn up by the Commission following a	<b>AM 76</b>  1.  The European Parliament and the Council shall appoint the European Data Protection Supervisor by common accord for a term of five	1.  The European Parliament and the Council shall appoint the European Data Protection Supervisor by common accord for a term of five years, on the basis of a list drawn up by the Commission following a	1.  The European Parliament and the Council shall appoint the European Data Protection Supervisor by common accord for a term of five years, on the basis of a list drawn up by the

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
public call for candidates. The call for candidates shall enable all interested parties throughout the Union to submit their applications. The list of candidates drawn up by the Commission shall be public. On the basis of the list drawn up by the Commission, the competent committee of the European Parliament may decide to hold a hearing in order to enable it to express a preference.	years, on the basis of a list drawn up <i>jointly</i> by the <b>European Parliament, the Council and the Commission</b> following a public call for candidates. The call for candidates shall enable all interested parties throughout the Union to submit their applications. The list of candidates drawn up by the Commission shall be public, <del>and</del> <b>shall consist of at least five candidates.</b> <del>On the basis of the list drawn up by the Commission,</del> The competent committee of the European Parliament may decide to hold a hearing <b>of the listed candidates</b> in order to enable it to express a preference.	public call for candidates. The call for candidates shall enable all interested parties throughout the Union to submit their applications. The list of candidates drawn up by the Commission shall be public. On the basis of the list drawn up by the Commission, the competent committee of the European Parliament may decide to hold a hearing in order to enable it to express a preference.	Commission following a public call for candidates. The call for candidates shall enable all interested parties throughout the Union to submit their applications. The list of candidates drawn up by the Commission shall be public and shall consist of at least three candidates. On the basis of the list drawn up by the Commission, the competent committee of the European Parliament may decide to hold a hearing in order to enable it to express a preference.
2.  The list drawn up by the Commission from which the European Data Protection Supervisor shall be chosen shall be made up of persons whose independence is beyond doubt and who are acknowledged as having the experience and skills required to perform the duties of European Data	<b>AM 77</b>  2.  The list drawn up <i>jointly</i> by the <b>European Parliament, the Council and the Commission</b> from which the European Data Protection Supervisor shall be chosen shall be made up of persons whose independence is beyond doubt and	2.  The list drawn up by the Commission from which the European Data Protection Supervisor shall be chosen shall be made up of persons whose independence is beyond doubt and who are acknowledged as having the experience and skills required to perform the duties of European	2.  The list drawn up by the Commission from which the European Data Protection Supervisor shall be chosen shall be made up of persons whose independence is beyond doubt and who are acknowledged as having expert knowledge in data protection as well as the

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
Protection Supervisor, for example because they belong or have belonged to the supervisory authorities established under Article 41 of Regulation (EU) 2016/679.	who are acknowledged as having <i>expert knowledge in data protection as well as</i> the experience and skills required to perform the duties of European Data Protection Supervisor, for example because they belong or have belonged to the supervisory authorities established under Article 41 of Regulation (EU) 2016/679.	Data Protection Supervisor, <del>for example because they belong or have belonged to the supervisory authorities established under Article 41 of Regulation (EU) 2016/679.</del>	experience and skills required to perform the duties of European Data Protection Supervisor.
3.  The term of office of the European Data Protection Supervisor shall be renewable once.	3.  The term of office of the European Data Protection Supervisor shall be renewable once.	3.  The term of office of the European Data Protection Supervisor shall be renewable once.	
4.  The duties of the European Data Protection Supervisor shall cease in the following circumstances:	4.  The duties of the European Data Protection Supervisor shall cease in the following circumstances:	4.  The duties of the European Data Protection Supervisor shall cease in the following circumstances:	
(a)  if the European Data Protection Supervisor is replaced;	(a)  if the European Data Protection Supervisor is replaced;	(a)  if the European Data Protection Supervisor is replaced;	
(b)	(b)	(b)	



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
if the European Data Protection Supervisor resigns;	if the European Data Protection Supervisor resigns;	if the European Data Protection Supervisor resigns;	
(c) if the European Data Protection Supervisor is dismissed or required to take compulsory retirement.	(c) if the European Data Protection Supervisor is dismissed or required to take compulsory retirement.	(c) if the European Data Protection Supervisor is dismissed or required to take compulsory retirement.	
5.  The European Data Protection Supervisor may be dismissed or deprived of his or her right to a pension or other benefits in its stead by the Court of Justice of the European Union at the request of the European Parliament, the Council or the Commission, if he or she no longer fulfils the conditions required for the performance of his or her duties or if he or she is guilty of serious misconduct.	5.  The European Data Protection Supervisor may be dismissed or deprived of his or her right to a pension or other benefits in its stead by the Court of Justice of the European Union at the request of the European Parliament, the Council or the Commission, if he or she no longer fulfils the conditions required for the performance of his or her duties or if he or she is guilty of serious misconduct.	5.  The European Data Protection Supervisor may be dismissed or deprived of his or her right to a pension or other benefits in its stead by the Court of Justice of the European Union at the request of the European Parliament, the Council or the Commission, if he or she no longer fulfils the conditions required for the performance of his or her duties or if he or she is guilty of serious misconduct.	
6.  In the event of normal replacement or voluntary resignation, the European Data Protection	6.  In the event of normal replacement or voluntary resignation, the European Data Protection	6.  In the event of normal replacement or voluntary resignation, the European Data Protection	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
Supervisor shall nevertheless remain in office until he or she has been replaced.	Supervisor shall nevertheless remain in office until he or she has been replaced.	Supervisor shall nevertheless remain in office until he or she has been replaced.	
7.  Articles 11 to 14 and 17 of the Protocol on the Privileges and Immunities of the European Union shall apply to the European Data Protection Supervisor.	7.  Articles 11 to 14 and 17 of the Protocol on the Privileges and Immunities of the European Union shall apply to the European Data Protection Supervisor.	7.  Articles 11 to 14 and 17 of the Protocol on the Privileges and Immunities of the European Union shall apply to the European Data Protection Supervisor.	
<i>Article 55</i>	<i>Article 55</i>	<i>Article 55</i>	
<i>Regulations and general conditions governing the performance of the European Data Protection Supervisor's duties, staff and financial resources</i>	<i>Regulations and general conditions governing the performance of the European Data Protection Supervisor's duties, staff and financial resources</i>	<i>Regulations and general conditions governing the performance of the European Data Protection Supervisor's duties, staff and financial resources</i>	
1.  The European Data Protection Supervisor shall be considered equivalent to a judge of the Court of Justice of the European Union as regards the determination of remuneration, allowances, retirement pension and any other benefit in lieu	1.  The European Data Protection Supervisor shall be considered equivalent to a judge of the Court of Justice of the European Union as regards the determination of remuneration, allowances, retirement pension and any other benefit in lieu	1.  The European Data Protection Supervisor shall be considered equivalent to a judge of the Court of Justice of the European Union as regards the determination of remuneration, allowances, retirement pension and any other benefit in lieu	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
of remuneration.	of remuneration.	of remuneration.	
<p>2.</p> <p>The budget authority shall ensure that the European Data Protection Supervisor is provided with the human and financial resources necessary for the performance of his or her tasks.</p>	<p>2.</p> <p>The budget authority shall ensure that the European Data Protection Supervisor is provided with the human and financial resources necessary for the performance of his or her tasks.</p>	<p>2.</p> <p>The budget authority shall ensure that the European Data Protection Supervisor is provided with the human and financial resources necessary for the performance of his or her tasks.</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>3.</p> <p>The budget of the European Data Protection Supervisor shall be shown in a separate budget heading in Section IX of the general budget of the European Union.</p>	<p>3.</p> <p>The budget of the European Data Protection Supervisor shall be shown in a separate budget heading in Section IX of the general budget of the European Union.</p>	<p>3.</p> <p>The budget of the European Data Protection Supervisor shall be shown in a separate budget heading in Section IX of the general budget of the European Union.</p>	
<p>4.</p> <p>The European Data Protection Supervisor shall be assisted by a Secretariat. The officials and other staff members of the Secretariat shall be appointed by the European Data Protection Supervisor and their superior shall be the European Data Protection Supervisor. They shall be subject exclusively to his or her direction. Their numbers shall be decided each year as part of the budgetary procedure.</p>	<p><b>AM 78</b></p> <p>4.</p> <p>The European Data Protection Supervisor shall be assisted by a Secretariat. The officials and other staff members of the Secretariat shall be appointed by the European Data Protection Supervisor and their superior shall be the European Data Protection Supervisor. They shall be subject exclusively to his or her direction. Their numbers shall be decided each year as part of the budgetary procedure. <i>Article 75(2) of Regulation (EU) 2016/679 shall apply to the staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the European Data</i></p>	<p>4.</p> <p>The European Data Protection Supervisor shall be assisted by a Secretariat. The officials and other staff members of the Secretariat shall be appointed by the European Data Protection Supervisor and their superior shall be the European Data Protection Supervisor. They shall be subject exclusively to his or her direction, <b>except wherethey are members of the secretariat to the European Data Protection Board in accordance with Article 75 of Regulation (EU) 2016/679.</b> Their numbers shall be decided each year as part of the budgetary procedure.</p>	<p>4. The European Data Protection Supervisor shall be assisted by a Secretariat. The officials and other staff members of the Secretariat shall be appointed by the European Data Protection Supervisor and their superior shall be the European Data Protection Supervisor. They shall be subject exclusively to his or her direction. Their numbers shall be decided each year as part of the budgetary procedure. Article 75(2) of Regulation (EU) 2016/679 shall apply to the staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the European Data Protection Board by Union law.</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>Protection Board by Union law.</i>		
<p>5.</p> <p>The officials and the other staff members of the Secretariat of the European Data Protection Supervisor shall be subject to the rules and regulations applicable to officials and other servants of the European Union.</p>	<p>5.</p> <p>The officials and the other staff members of the Secretariat of the European Data Protection Supervisor shall be subject to the rules and regulations applicable to officials and other servants of the European Union.</p>	<p>5.</p> <p>The officials and the other staff members of the Secretariat of the European Data Protection Supervisor shall be subject to the rules and regulations applicable to officials and other servants of the European Union.</p>	
<p>6.</p> <p>The European Data Protection Supervisor shall have its seat in Brussels.</p>	<p>6.</p> <p>The European Data Protection Supervisor shall have its seat in Brussels.</p>	<p>6.</p> <p>The European Data Protection Supervisor shall have its seat in Brussels.</p>	
<i>Article 56</i>	<i>Article 56</i>	<i>Article 56</i>	
<i>Independence</i>	<i>Independence</i>	<i>Independence</i>	
<p>1.</p> <p>The European Data Protection Supervisor shall act with complete independence in performing his or her tasks and exercising his or her powers in accordance with this Regulation.</p>	<p>1.</p> <p>The European Data Protection Supervisor shall act with complete independence in performing his or her tasks and exercising his or her powers in accordance with this Regulation.</p>	<p>1.</p> <p>The European Data Protection Supervisor shall act with complete independence in performing his or her tasks and exercising his or her powers in accordance with this Regulation.</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>2.</p> <p>The European Data Protection Supervisor shall, in the performance of his or her tasks and exercise of his or her powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.</p>	<p>2.</p> <p>The European Data Protection Supervisor shall, in the performance of his or her tasks and exercise of his or her powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.</p>	<p>2.</p> <p>The European Data Protection Supervisor shall, in the performance of his or her tasks and exercise of his or her powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.</p>	
<p>3.</p> <p>The European Data Protection Supervisor shall refrain from any action incompatible with his or her duties and shall not, during his or her term of office, engage in any other occupation, whether gainful or not.</p>	<p>3.</p> <p>The European Data Protection Supervisor shall refrain from any action incompatible with his or her duties and shall not, during his or her term of office, engage in any other occupation, whether gainful or not.</p>	<p>3.</p> <p>The European Data Protection Supervisor shall refrain from any action incompatible with his or her duties and shall not, during his or her term of office, engage in any other occupation, whether gainful or not.</p>	
<p>4.</p> <p>The European Data Protection Supervisor shall, after his or her term of office, behave with integrity and discretion as regards the acceptance of appointments and</p>	<p>4.</p> <p>The European Data Protection Supervisor shall, after his or her term of office, behave with integrity and discretion as regards the acceptance of appointments and</p>	<p>4.</p> <p>The European Data Protection Supervisor shall, after his or her term of office, behave with integrity and discretion as regards the acceptance of appointments</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
benefits.	benefits.	and benefits.	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<i>Article 57</i>	<i>Article 57</i>	<i>Article 57</i>	
<i>Professional secrecy</i>	<i>Professional secrecy</i>	<i>Professional secrecy</i>	
The European Data Protection Supervisor and his or her staff shall, both during and after their term of office, be subject to a duty of professional secrecy with regard to any confidential information which has come to their knowledge in the course of the performance of their official duties.	The European Data Protection Supervisor and his or her staff shall, both during and after their term of office, be subject to a duty of professional secrecy with regard to any confidential information which has come to their knowledge in the course of the performance of their official duties.	The European Data Protection Supervisor and his or her staff shall, both during and after their term of office, be subject to a duty of professional secrecy with regard to any confidential information which has come to their knowledge in the course of the performance of their official duties.	
<i>Article 58</i>	<i>Article 58</i>	<i>Article 58</i>	
<i>Tasks</i>	<i>Tasks</i>	<i>Tasks</i>	
1.  Without prejudice to other tasks set out under this Regulation, the European Data Protection Supervisor shall:	1.  Without prejudice to other tasks set out under this Regulation, the European Data Protection Supervisor shall:	1.  Without prejudice to other tasks set out under this Regulation, the European Data Protection Supervisor shall:	
(a)  monitor and enforce the application of this Regulation and other Union acts relating to the protection of	(a)  monitor and enforce the application of this Regulation and other Union acts relating to the protection of	(a)  monitor and enforce the application of this Regulation <del>and other Union acts relating to the</del>	(a) monitor and enforce the application of this by a Union institution or body, with the exception of the processing of personal data by the Court of



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
natural persons with regard to the processing of personal data by a Union institution or body, with the exception of the processing of personal data by the Court of Justice of the European Union acting in its judicial capacity;	natural persons with regard to the processing of personal data by a Union institution or body, with the exception of the processing of personal data by the Court of Justice of the European Union acting in its judicial capacity;	<del>protection of natural persons with regard to the processing of personal data</del> by a Union institution or body, with the exception of the processing of personal data by the Court of Justice of the European Union acting in its judicial capacity;	Justice of the European Union acting in its judicial capacity;
(b)  promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;	(b)  promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;	(b)  promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;	
(c)  promote the awareness of controllers and processors of their obligations under this Regulation;	(c)  promote the awareness of controllers and processors of their obligations under this Regulation;	(c)  promote the awareness of controllers and processors of their obligations under this Regulation;	
(d)  upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate,	(d)  upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate,	(d)  upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate,	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
cooperate with the supervisory authorities in Member States to that end;	cooperate with the supervisory authorities in Member States to that end;	cooperate with the supervisory authorities in Member States to that end;	
(e)  handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 67, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;	(e)  handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 67, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;	(e)  handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 67, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;	
(f)  conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;	(f)  conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;	(f)  conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;	
(g)	(g)	(g)	(g) advise, on its own initiative or

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
advise all Union institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to the processing of personal data;	advise all Union institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to the processing of personal data;	advise, <b>on its own initiative or on request</b> , all Union institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to the processing of personal data;	on request, all Union institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to the processing of personal data;
(h)  monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies;	(h)  monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies;	(h)  monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies;	
(i)  adopt standard contractual clauses referred to in Article 29(8) and in point (c) of Article 49(2);	(i)  adopt standard contractual clauses referred to in Article 29(8) and in point (c) of Article 49(2);	(i)  adopt standard contractual clauses referred to in Article 29(8) and in point (c) of Article 49(2);	
(j)  establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 39(4);	(j)  establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 39(4);	(j)  establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 39(4);	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
(k) participate in the activities of the European Data Protection Board set up by Article 68 of Regulation (EU) 2016/679;	(k) participate in the activities of the European Data Protection Board set up by Article 68 of Regulation (EU) 2016/679;	(k) participate in the activities of the European Data Protection Board set up by Article 68 of Regulation (EU) 2016/679;	
(l) provide the secretariat for the European Data Protection Board, in accordance with Article 75 of Regulation (EU) 2016/679;	(l) provide the secretariat for the European Data Protection Board, in accordance with Article 75 of Regulation (EU) 2016/679;	(l) provide the secretariat for the European Data Protection Board, in accordance with Article 75 of Regulation (EU) 2016/679;	
(m) give advice on the processing referred to in Article 40(2);	(m) give advice on the processing referred to in Article 40(2);	(m) give advice on the processing referred to in Article 40(2);	
(n) authorise contractual clauses and provisions referred to in Article 49(3);	(n) authorise contractual clauses and provisions referred to in Article 49(3);	(n) authorise contractual clauses and provisions referred to in Article 49(3);	
(o) keep internal records of infringements of this Regulation and of measures taken in accordance	(o) keep internal records of infringements of this Regulation and of measures taken in accordance	(o) keep internal records of infringements of this Regulation and of measures taken in	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
with Article 59(2);	with Article 59(2);	accordance with Article 59(2);	
(p) fulfil any other tasks related to the protection of personal data; and	(p) fulfil any other tasks related to the protection of personal data; and	(p) fulfil any other tasks related to the protection of personal data; and	
(q) establish his or her Rules of Procedure.	(q) establish his or her Rules of Procedure.	(q) establish his or her Rules of Procedure.	
2.  The European Data Protection Supervisor shall facilitate the submission of complaints referred to in point (e) of paragraph 1 by a complaint submission form which can also be completed electronically, without excluding other means of communication.	2.  The European Data Protection Supervisor shall facilitate the submission of complaints referred to in point (e) of paragraph 1 by a complaint submission form which can also be completed electronically, without excluding other means of communication.	2.  The European Data Protection Supervisor shall facilitate the submission of complaints referred to in point (e) of paragraph 1 by a complaint submission form which can also be completed electronically, without excluding other means of communication.	
3.  The performance of the tasks of the European Data Protection Supervisor shall be free of charge for the data subject.	3.  The performance of the tasks of the European Data Protection Supervisor shall be free of charge for the data subject.	3.  The performance of the tasks of the European Data Protection Supervisor shall be free of charge for the data subject.	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>4.</p> <p>Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the European Data Protection Supervisor may refuse to act on the request. The European Data Protection Supervisor shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.</p>	<p>4.</p> <p>Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the European Data Protection Supervisor may refuse to act on the request. The European Data Protection Supervisor shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.</p>	<p>4.</p> <p>Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the European Data Protection Supervisor may refuse to act on the request. The European Data Protection Supervisor shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.</p>	
<i>Article 59</i>	<i>Article 59</i>	<i>Article 59</i>	
<i>Powers</i>	<i>Powers</i>	<i>Powers</i>	
<p>1.</p> <p>The European Data Protection Supervisor shall have the following investigative powers:</p>	<p>1.</p> <p>The European Data Protection Supervisor shall have the following investigative powers:</p>	<p>1.</p> <p>The European Data Protection Supervisor shall have the following investigative powers:</p>	
<p>(a)</p> <p>to order the controller and the processor to provide any information it requires for the performance of its tasks;</p>	<p>(a)</p> <p>to order the controller and the processor to provide any information it requires for the performance of its tasks;</p>	<p>(a)</p> <p>to order the controller and the processor to provide any information it requires for the performance of its tasks;</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
		performance of its tasks;	
(b) to carry out investigations in the form of data protection audits;	(b) to carry out investigations in the form of data protection audits;	(b) to carry out investigations in the form of data protection audits;	
(c) to notify the controller or the processor of an alleged infringement of this Regulation;	(c) to notify the controller or the processor of an alleged infringement of this Regulation;	(c) to notify the controller or the processor of an alleged infringement of this Regulation;	
(d) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;	(d) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;	(d) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;	
(e) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law;	<b>AM 79</b> (e) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member	(e) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union <del>or Member State procedural</del> law;	(e) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union law;

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<del>State procedural law;</del>		
2.  The European Data Protection Supervisor shall have the following corrective powers:	2.  The European Data Protection Supervisor shall have the following corrective powers:	2.  The European Data Protection Supervisor shall have the following corrective powers:	
(a)  to issue warnings to a controller or processor that the intended processing operations are likely to infringe provisions of this Regulation;	(a)  to issue warnings to a controller or processor that the intended processing operations are likely to infringe provisions of this Regulation;	(a)  to issue warnings to a controller or processor that the intended processing operations are likely to infringe provisions of this Regulation;	
(b)  to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;	(b)  to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;	(b)  to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;	
(c)  refer the matter to the controller or processor concerned and, if necessary, to the European Parliament, the Council and the Commission;	(c)  refer the matter to the controller or processor concerned and, if necessary, to the European Parliament, the Council and the Commission;	(c)  refer the matter to the controller or processor concerned and, if necessary, to the European Parliament, the Council and the Commission;	



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
(d) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;	(d) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;	(d) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;	
(e) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;	(e) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;	(e) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;	
(f) to order the controller to communicate a personal data breach to the data subject;	(f) to order the controller to communicate a personal data breach to the data subject;	(f) to order the controller to communicate a personal data breach to the data subject;	
(g) to impose a temporary or definitive limitation including a ban on processing;	(g) to impose a temporary or definitive limitation including a ban on processing;	(g) to impose a temporary or definitive limitation including a ban on processing;	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
(h) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 18, 19 and 20 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 19(2) and Article 21;	(h) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 18, 19 and 20 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 19(2) and Article 21;	(h) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 18, 19 and 20 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 19(2) and Article 21;	
(i) to impose an administrative fine pursuant to Article 66, subject to non-compliance by the Union institution or body with one of the measures referred to in this paragraph and depending on the circumstances of each individual case;	(i) to impose an administrative fine pursuant to Article 66, subject to non-compliance by the Union institution or body with one of the measures referred to in this paragraph and depending on the circumstances of each individual case;	(i) to impose an administrative fine pursuant to Article 66, <b>in the case of subject to</b> non-compliance by the Union institution or body with one of the measures referred to <b>points (d) to (h) and (j) of in</b> this paragraph and depending on the circumstances of each individual case;	(i) to impose an administrative fine pursuant to Article 66, in the case of non-compliance by the Union institution or body with one of the measures referred to points (d) to (h) and (j) of this paragraph and depending on the circumstances of each individual case;
(j) to order the suspension of data flows to a recipient in a Member State, a third country or to an international organisation.	(j) to order the suspension of data flows to a recipient in a Member State, a third country or to an international organisation.	(j) to order the suspension of data flows to a recipient in a Member State, a third country or to an international organisation.	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
3.  The European Data Protection Supervisor shall have the following authorisation and advisory powers:	3.  The European Data Protection Supervisor shall have the following authorisation and advisory powers:	3.  The European Data Protection Supervisor shall have the following authorisation and advisory powers:	
(a)  to advise data subjects in the exercise of their rights;	(a)  to advise data subjects in the exercise of their rights;	(a)  to advise data subjects in the exercise of their rights;	
(b)  to advise the controller in accordance with the prior consultation procedure referred to in Article 40;	(b)  to advise the controller in accordance with the prior consultation procedure referred to in Article 40;	(b)  to advise the controller in accordance with the prior consultation procedure referred to in Article 40;	
	<b>AM 80</b>  <i>(ba)</i>  <i>to authorise or not the processing operations as referred to in Article 40(4);</i>		deletion
(c)  to issue, on its own initiative or on request, opinions to the Union	(c)  to issue, on its own initiative or on request, opinions to the Union	(c)  to issue, on its own initiative or on request, opinions to the Union	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
institutions and bodies and to the public on any issue related to the protection of personal data;	institutions and bodies and to the public on any issue related to the protection of personal data;	institutions and bodies and to the public on any issue related to the protection of personal data;	
(d) to adopt standard data protection clauses referred to in Article 29(8) and in point (c) of Article 49(2);	(d) to adopt standard data protection clauses referred to in Article 29(8) and in point (c) of Article 49(2);	(d) to adopt standard data protection clauses referred to in Article 29(8) and in point (c) of Article 49(2);	
(e) to authorise contractual clauses referred to in point (a) of Article 49(3);	(e) to authorise contractual clauses referred to in point (a) of Article 49(3);	(e) to authorise contractual clauses referred to in point (a) of Article 49(3);	
(f) to authorise administrative arrangements referred to in point (b) of Article 49(3);	(f) to authorise administrative arrangements referred to in point (b) of Article 49(3);	(f) to authorise administrative arrangements referred to in point (b) of Article 49(3);	
		(g) <b>to authorise processing operations pursuant to implementing acts based on Article 40(4).</b>	(g) to authorise processing operations or not pursuant to implementing acts based on Article 40(4);
4.	4.	4.	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
The exercise of the powers conferred on the European Data Protection Supervisor pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union law.	The exercise of the powers conferred on the European Data Protection Supervisor pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union law.	The exercise of the powers conferred on the European Data Protection Supervisor pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union law.	
5.  The European Data Protection Supervisor shall have the power to refer the matter to the Court of Justice of the European Union under the conditions provided for in the Treaty and to intervene in actions brought before the Court of Justice of the European Union.	5.  The European Data Protection Supervisor shall have the power to refer the matter to the Court of Justice of the European Union under the conditions provided for in the Treaty and to intervene in actions brought before the Court of Justice of the European Union.	5.  The European Data Protection Supervisor shall have the power to refer the matter to the Court of Justice of the European Union under the conditions provided for in the Treaty and to intervene in actions brought before the Court of Justice of the European Union.	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<i>Article 60</i>	<i>Article 60</i>	<i>Article 60</i>	
<i>Activities report</i>	<i>Activities report</i>	<i>Activities report</i>	
1.  The European Data Protection Supervisor shall submit an annual report on its activities to the European Parliament, the Council and the Commission and at the same time make it public.	1.  The European Data Protection Supervisor shall submit an annual report on its activities to the European Parliament, the Council and the Commission and at the same time make it public.	1.  The European Data Protection Supervisor shall submit an annual report on its activities to the European Parliament, the Council and the Commission and at the same time make it public.	
2.  The European Data Protection Supervisor shall forward the activities report to the other Union institutions and bodies, which may submit comments with a view to possible examination of the report in the European Parliament.	2.  The European Data Protection Supervisor shall forward the activities report to the other Union institutions and bodies, which may submit comments with a view to possible examination of the report in the European Parliament.	2.  The European Data Protection Supervisor shall forward the activities report to the other Union institutions and bodies, which may submit comments with a view to possible examination of the report in the European Parliament.	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<b>CHAPTER VII</b> <b>COOPERATION AND</b> <b>CONSISTENCY</b>	<b>CHAPTER VII</b> <b>COOPERATION AND</b> <b>CONSISTENCY</b>	<b>CHAPTER VII</b> <b>COOPERATION AND</b> <b>CONSISTENCY</b>	
<i>Article 61</i>	<i>Article 61</i>	<i>Article 61</i>	
<i>Cooperation with national supervisory authorities</i>	<b>AM 81</b>  Cooperation <del>with</del> <i>between the European Data Protection Supervisor and</i> national supervisory authorities	<i>Cooperation with national supervisory authorities</i>	<i>Cooperation between the European Data Protection Supervisor and national supervisory authorities</i>
The European Data Protection Supervisor shall cooperate with supervisory authorities established under Article 41 of Regulation (EU) 2016/679 and Article 51 of Directive (EU) 2016/680 (hereinafter “national supervisory authorities”) and with the joint supervisory authority established under Article 25 of Council Decision 2009/917/JHA <sup>12</sup> to the extent necessary for the performance of their respective	<b>AM 82</b>  The European Data Protection Supervisor shall cooperate with supervisory authorities established under Article <del>41</del> <sup>51</sup> of Regulation (EU) 2016/679 and Article <del>51</del> <sup>41</sup> of Directive (EU) 2016/680 (hereinafter “national supervisory authorities”) <del>and with the joint supervisory authority established under Article 25 of Council Decision 2009/917/JHA<sup>13</sup> to the</del>	The European Data Protection Supervisor shall cooperate with supervisory authorities established under Article 41 of Regulation (EU) 2016/679 and Article 51 of Directive (EU) 2016/680 (hereinafter “national supervisory authorities”) and with the joint supervisory authority established under Article 25 of Council Decision 2009/917/JHA <sup>12</sup> to the extent necessary for the performance of their respective	The European Data Protection Supervisor shall cooperate with supervisory authorities established under Article 51 of Regulation (EU) 2016/679 and Article 41 of Directive (EU) 2016/680 (hereinafter “national supervisory authorities”) and with the joint supervisory authority established under Article 25 of Council Decision 2009/917/JHA <sup>12</sup> to the extent necessary for the performance of their respective

<sup>12</sup> Council Decision 2009/917/JHA of 30 November 2009 on the use of information technology for customs purposes, OJ L 323, 10.12.2009, p. 20–30.

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
duties, in particular by providing each other with relevant information, requesting national supervisory authorities to exercise their powers or responding to a request from such authorities.	<p>extent necessary for the performance of their respective duties, in particular by providing each other with relevant information, requesting <del>national supervisory authorities</del> <b>each other</b> to exercise their powers or responding to <del>a request from such authorities</del> <b>each other's requests</b>.</p> <hr/> <p><sup>13</sup> <del>Council Decision 2009/917/JHA of 30 November 2009 on the use of information technology for customs purposes, OJ L 323, 10.12.2009, p. 20–30.</del></p>	duties, in particular by providing each other with relevant information, requesting national supervisory authorities to exercise their powers or responding to a request from such authorities.	duties, in particular by providing each other with relevant information, requesting each other to exercise their powers or responding each other requests.
	<p><b>AM 83</b></p> <p><i>1a. The European Data Protection Supervisor and the European Data Protection Board may use the Internal Market Information System established by Regulation (EU) No 1024/2012 of the European Parliament and of the Council of 25 October 2012 on administrative cooperation through the Internal Market Information System and repealing Commission</i></p>		deletion



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>Decision 2008/49/EC ('the IMI Regulation') for the purposes of administrative cooperation and information exchange pursuant to Articles 60 to 62, 64, 65 and 70 of Regulation (EU) 2016/679.</i>		
<i>Article 62</i>	<i>Article 62</i>	<i>Article 62</i>	<i>Article 62</i>
<i>Coordinated supervision by the European Data Protection Supervisor and national supervisory authorities</i>	<i>Coordinated supervision by the European Data Protection Supervisor and national supervisory authorities</i>	<i>Coordinated supervision by the European Data Protection Supervisor and national supervisory authorities</i>	<i>Coordinated supervision by the European Data Protection Supervisor and national supervisory authorities</i>
<p>1.</p> <p>Where a Union act refers to this Article, the European Data Protection Supervisor shall cooperate actively with the national supervisory authorities, in order to ensure effective supervision of large IT systems or Union agencies.</p>	<p><b>AM 84</b></p> <p>1.</p> <p>Where a Union act <del>refers to this Article,</del> <b>envisages that</b> the European Data Protection Supervisor <del>shall cooperate actively with the</del> <b>supervises the processing of personal data at Union level and national supervisory authorities supervise the processing of personal data at national level, the European Data Protection Supervisor and the national supervisory authorities, each acting</b></p>	<p>1.</p> <p>Where a Union act refers to this Article, the European Data Protection Supervisor shall cooperate actively with the national supervisory authorities, in order to ensure effective supervision of large IT systems or Union <b>bodies, offices and</b> agencies.</p>	<p>1. Where a Union act refers to this Article, the European Data Protection Supervisor and the national supervisory authorities, each acting within the scope of their respective competencies, shall cooperate actively in the framework of their responsibilities in order to ensure effective supervision of large IT systems or Union bodies, offices and agencies.</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>within the scope of their respective competencies, shall cooperate actively in the framework of their responsibilities</i> in order to ensure effective <i>coordinated supervision of</i> large IT systems or Union <i>bodies, offices or</i> agencies.		
<p>2.</p> <p>The European Data Protection Supervisor shall, acting within the scope of its respective competences and in the framework of its responsibilities, exchange relevant information, assist in carrying out audits and inspections, examine difficulties of interpretation or application of this Regulation and other applicable Union acts, study problems with the exercise of independent supervision or in the exercise of the rights of data subjects, draw up harmonised proposals for solutions to any problems and promote awareness of data protection rights, as necessary, jointly with the national supervisory authorities.</p>	<p><b>AM 85</b></p> <p>2.</p> <p><del>The European Data Protection Supervisor</del> <i>They</i> shall, <i>each</i> acting within the scope of <del>its</del> <i>their</i> respective competences and in the framework of <del>its</del> <i>their</i> responsibilities, exchange relevant information, assist <i>each other</i> in carrying out audits and inspections, examine difficulties of interpretation or application of this Regulation and other applicable Union acts, study problems with the exercise of independent supervision or in the exercise of the rights of data subjects, draw up harmonised proposals for solutions to any problems and promote awareness of data protection rights, as necessary, <del>jointly with the national supervisory authorities.</del></p>	<p>2.</p> <p>The European Data Protection Supervisor shall, acting within the scope of its respective competences and in the framework of its responsibilities, exchange relevant information, assist in carrying out audits and inspections, examine difficulties of interpretation or application of this Regulation and other applicable Union acts, study problems with the exercise of independent supervision or in the exercise of the rights of data subjects, draw up harmonised proposals for solutions to any problems and promote awareness of data protection rights, as necessary, jointly with the national supervisory authorities.</p>	<p>2. They shall, each acting within the scope of their respective competences and in the framework of -their responsibilities, exchange relevant information, assist each other in carrying out audits and inspections, examine difficulties of interpretation or application of this Regulation and other applicable Union acts, study problems with the exercise of independent supervision or in the exercise of the rights of data subjects, draw up harmonised proposals for solutions to any problems and promote awareness of data protection rights, as necessary.</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<p>3.</p> <p>For the purposes laid down in paragraph 2, the European Data Protection Supervisor shall meet <i>with</i> the national supervisory authorities at least twice a year within the framework of the European Data Protection Board. The costs and servicing of those meetings shall be borne by the European Data Protection Board. Rules of procedure shall be adopted at the first meeting. Further working methods shall be developed jointly as necessary.</p>	<p><b>AM 86</b></p> <p>3.</p> <p>For the purposes laid down in paragraph 2, the European Data Protection Supervisor <del>shall meet with</del> <b>and</b> the national supervisory authorities <b>shall meet</b> at least twice a year within the framework of the European Data Protection Board. The costs and servicing of those meetings shall be borne by the European Data Protection Board. <del>Rules of procedure shall be adopted at the first meeting.</del> <b>For these purposes, the European Data Protection Board may develop further working methods</b> <del>shall be developed jointly</del> as necessary.</p>	<p>3.</p> <p>For the purposes laid down in paragraph 2, the European Data Protection Supervisor shall meet with the national supervisory authorities at least twice a year within the framework of the European Data Protection Board. <del>The costs and servicing of those meetings shall be borne by the European Data Protection Board.</del> Rules of procedure shall be adopted at the first meeting. Further working methods shall be developed jointly as necessary.</p>	<p>3. For the purposes laid down in paragraph 2, the European Data Protection Supervisor and the national supervisory authorities shall meet at least twice a year within the framework of the European Data Protection Board. For these purposes, the European Data Protection Board may develop further working methods as necessary.</p>
<p>4.</p> <p>A joint report of activities as regard coordinated supervision shall be sent by the European Data Protection Board to the European Parliament, the Council, and the Commission every two years.</p>	<p>4.</p> <p>A joint report of activities as regard coordinated supervision shall be sent by the European Data Protection Board to the European Parliament, the Council, and the Commission every two years.</p>	<p>4.</p> <p>A joint report of activities as regard coordinated supervision shall be sent by the European Data Protection Board to the European Parliament, the Council, and the Commission every two years.</p>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<b>CHAPTER VIII</b> <b>REMEDIES, LIABILITY AND PENALTIES</b>	<b>CHAPTER VIII</b> <b>REMEDIES, LIABILITY AND PENALTIES</b>	<b>CHAPTER VIII</b> <b>REMEDIES, LIABILITY AND PENALTIES</b>	
<i>Article 63</i>	<i>Article 63</i>	<i>Article 63</i>	
<i>Right to lodge a complaint with the European Data Protection Supervisor</i>	<i>Right to lodge a complaint with the European Data Protection Supervisor</i>	<i>Right to lodge a complaint with the European Data Protection Supervisor</i>	
1.  Without prejudice to any judicial, administrative or non-judicial remedy, every data subject shall have the right to lodge a complaint with the European Data Protection Supervisor if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.	1.  Without prejudice to any judicial, administrative or non-judicial remedy, every data subject shall have the right to lodge a complaint with the European Data Protection Supervisor if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.	1.  Without prejudice to any judicial, administrative or non-judicial remedy, every data subject shall have the right to lodge a complaint with the European Data Protection Supervisor if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.	
2.  The European Data Protection Supervisor shall inform the data subject of the progress and the	2.  The European Data Protection Supervisor shall inform the data subject of the progress and the	2.  The European Data Protection Supervisor shall inform the data subject of the progress and the	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
outcome of the complaint, including of the possibility of a judicial remedy pursuant to Article 64.	outcome of the complaint, including of the possibility of a judicial remedy pursuant to Article 64.	outcome of the complaint, including of the possibility of a judicial remedy pursuant to Article 64.	
3.  If the European Data Protection Supervisor does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint, the complaint shall be deemed to have been rejected.	3.  If the European Data Protection Supervisor does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint, the complaint shall be deemed to have been rejected.	3.  If the European Data Protection Supervisor does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint, the <b>European Data Protection Supervisor complaint</b> shall be deemed to have <b>adopted a negative decision</b> <del>been rejected</del> .	3. If the European Data Protection Supervisor does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint, the European Data Protection Supervisor shall be deemed to have adopted a negative decision.
<i>Article 64</i>	<i>Article 64</i>	<i>Article 64</i>	
<i>Right to an effective judicial remedy</i>	<i>Right to an effective judicial remedy</i>	<i>Right to an effective judicial remedy</i>	
		1.  <b>Actions against decisions of the European Data Protection Supervisor, including decisions referred to in Article 63(3), shall be brought before the Court of Justice of the European Union.</b>	1. The Court of Justice of the European Union shall have jurisdiction to hear all disputes relative to the provisions of this Regulation, including claims for damages.

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
The Court of Justice of the European Union shall have jurisdiction to hear all disputes relative to the provisions of this Regulation, including claims for damages.	The Court of Justice of the European Union shall have jurisdiction to hear all disputes relative to the provisions of this Regulation, including claims for damages.	2.  The Court of Justice of the European Union shall have jurisdiction to hear all disputes relative to the provisions of this Regulation, including claims for damages.	2. Actions against decisions of the European Data Protection Supervisor, including decisions referred to in Article 63(3), shall be brought before the Court of Justice of the European Union.
		3.  <b>The Court of Justice of the European Union shall have unlimited jurisdiction to review administrative fines referred to in Article 66. It may cancel, reduce or increase those fines within the limits of Article 66.</b>	3. The Court of Justice of the European Union shall have unlimited jurisdiction to review administrative fines referred to in Article 66. It may cancel, reduce or increase those fines within the limits of Article 66.
<i>Article 65</i>	<i>Article 65</i>	<i>Article 65</i>	
<i>Right to compensation</i>	<i>Right to compensation</i>	<i>Right to compensation</i>	
Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered, subject to the	Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered, subject to the	Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the <b>Union institution or body</b> <del>controller or processor</del> for the	Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the Union institution or body for the damage suffered, subject to

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
conditions provided for in the Treaties.	conditions provided for in the Treaties.	damage suffered, subject to the conditions provided for in the Treaties.	the conditions provided for in the Treaties.

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<i>Article 66</i>	<i>Article 66</i>	<i>Article 66</i>	
<i>Administrative fines</i>	<i>Administrative fines</i>	<i>Administrative fines</i>	
<p>1.</p> <p>The European Data Protection Supervisor may impose administrative fines on Union institutions and bodies, depending on the circumstances of each individual case, where a Union institution or body fails to comply with an order by the European Data Protection Supervisor pursuant to points (d) to (h) and (j) of Article 59(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:</p>	<p>1.</p> <p>The European Data Protection Supervisor may impose administrative fines on Union institutions and bodies, depending on the circumstances of each individual case, where a Union institution or body fails to comply with an order by the European Data Protection Supervisor pursuant to points (d) to (h) and (j) of Article 59(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:</p>	<p>1.</p> <p>The European Data Protection Supervisor may impose administrative fines on Union institutions and bodies, depending on the circumstances of each individual case, where a Union institution or body fails to comply with an order by the European Data Protection Supervisor pursuant to points (d) to (h) and (j) of Article 59(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:</p>	
<p>(a)</p> <p>the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the</p>	<p>(a)</p> <p>the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the</p>	<p>(a)</p> <p>the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing</p>	



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
number of data subjects affected and the level of damage suffered by them;	number of data subjects affected and the level of damage suffered by them;	concerned as well as the number of data subjects affected and the level of damage suffered by them;	
(b)  any action taken by the Union institution or body to mitigate the damage suffered by data subjects;	(b)  any action taken by the Union institution or body to mitigate the damage suffered by data subjects;	(b)  any action taken by the Union institution or body to mitigate the damage suffered by data subjects;	
(c)  the degree of responsibility of the Union institution or body taking into account technical and organisational measures implemented by them pursuant to Articles 27 and 33;	(c)  the degree of responsibility of the Union institution or body taking into account technical and organisational measures implemented by them pursuant to Articles 27 and 33;	(c)  the degree of responsibility of the Union institution or body taking into account technical and organisational measures implemented by them pursuant to Articles 27 and 33;	
(d)  any similar previous infringements by the Union institution or body;	(d)  any similar previous infringements by the Union institution or body;	(d)  any similar previous infringements by the Union institution or body;	
(e)  the degree of cooperation with the European Data Protection Supervisor, in order to remedy the infringement and mitigate the	(e)  the degree of cooperation with the European Data Protection Supervisor, in order to remedy the infringement and mitigate the	(e)  the degree of cooperation with the European Data Protection Supervisor, in order to remedy the infringement and mitigate the	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
possible adverse effects of the infringement;	possible adverse effects of the infringement;	possible adverse effects of the infringement;	
(f) the categories of personal data affected by the infringement;	(f) the categories of personal data affected by the infringement;	(f) the categories of personal data affected by the infringement;	
(g) the manner in which the infringement became known to the European Data Protection Supervisor, in particular whether, and if so to what extent, the Union institution or body notified the infringement;	(g) the manner in which the infringement became known to the European Data Protection Supervisor, in particular whether, and if so to what extent, the Union institution or body notified the infringement;	(g) the manner in which the infringement became known to the European Data Protection Supervisor, in particular whether, and if so to what extent, the Union institution or body notified the infringement;	
(h) where measures referred to in Article 59 have previously been ordered against the Union institution or body concerned with regard to the same subject-matter, compliance with those measures.	(h) where measures referred to in Article 59 have previously been ordered against the Union institution or body concerned with regard to the same subject-matter, compliance with those measures.	(h) where measures referred to in Article 59 have previously been ordered against the Union institution or body concerned with regard to the same subject-matter, compliance with those measures.	
The proceedings leading to the imposition of those fines should be carried out in a reasonable	The proceedings leading to the imposition of those fines should be carried out in a reasonable	The proceedings leading to the imposition of those fines should be carried out in a reasonable	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
timeframe according to the circumstances of the case and taking into account the relevant actions and proceedings referred to in Article 69.	timeframe according to the circumstances of the case and taking into account the relevant actions and proceedings referred to in Article 69.	timeframe according to the circumstances of the case and taking into account the relevant actions and proceedings referred to in Article 69.	
2.  Infringements of the obligations of the Union institution or body pursuant to Articles 8, 12 27, 28, 29, 30, 31, 32, 33, 37, 38, 39, 40, 44, 45 and 46 shall, in accordance with paragraph 1, be subject to administrative fines up to 25 000 EUR per infringement and up to a total of 250 000 EUR per year.	2.  Infringements of the obligations of the Union institution or body pursuant to Articles 8, 12 27, 28, 29, 30, 31, 32, 33, 37, 38, 39, 40, 44, 45 and 46 shall, in accordance with paragraph 1, be subject to administrative fines up to 25 000 EUR per infringement and up to a total of 250 000 EUR per year.	2.  Infringements of the obligations of the Union institution or body pursuant to Articles 8, 12, 27, 28, 29, 30, 31, 32, 33, 37, 38, 39, 40, 44, 45 and 46 shall, in accordance with paragraph 1, be subject to administrative fines up to 25 000 EUR per infringement and up to a total of 250 000 EUR per year.	
3.  Infringements of the following provisions by the Union institution or body shall, in accordance with paragraph 1, be subject to administrative fines up to 50 000 EUR per infringement and up to a total of 500 000 EUR per year:	3.  Infringements of the following provisions by the Union institution or body shall, in accordance with paragraph 1, be subject to administrative fines up to 50 000 EUR per infringement and up to a total of 500 000 EUR per year:	3.  Infringements of the following provisions by the Union institution or body shall, in accordance with paragraph 1, be subject to administrative fines up to 50 000 EUR per infringement and up to a total of 500 000 EUR per year:	
(a)	(a)	(a)	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
the basic principles for processing, including conditions for consent, pursuant to Articles 4, 5, 7 and 10;	the basic principles for processing, including conditions for consent, pursuant to Articles 4, 5, 7 and 10;	the basic principles for processing, including conditions for consent, pursuant to Articles 4, 5, 7 and 10;	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
(b) the data subjects' rights pursuant to Articles 14 to 24;	(b) the data subjects' rights pursuant to Articles 14 to 24;	(b) the data subjects' rights pursuant to Articles 14 to 24;	
(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 47 to 51.	(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 47 to 51.	(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 47 to 51.	
4. If a Union institution or body, for the same or linked or continuous processing operations, infringes several provisions of this Regulation or the same provision of this Regulation several times, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.	4. If a Union institution or body, for the same or linked or continuous processing operations, infringes several provisions of this Regulation or the same provision of this Regulation several times, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.	4. If a Union institution or body, for the same or linked or continuous processing operations, infringes several provisions of this Regulation or the same provision of this Regulation several times, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.	
5. Before taking decisions pursuant to this Article, the European Data Protection Supervisor shall give the	5. Before taking decisions pursuant to this Article, the European Data Protection Supervisor shall give the	5. Before taking decisions pursuant to this Article, the European Data Protection Supervisor shall give	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
Union institution or body which is the subject of the proceedings conducted by the Supervisor the opportunity of being heard on the matters to which the Supervisor has taken objection. The European Data Protection Supervisor shall base its decisions only on objections on which the parties concerned have been able to comment. Complainants shall be associated closely with the proceedings.	Union institution or body which is the subject of the proceedings conducted by the Supervisor the opportunity of being heard on the matters to which the Supervisor has taken objection. The European Data Protection Supervisor shall base its decisions only on objections on which the parties concerned have been able to comment. Complainants shall be associated closely with the proceedings.	the Union institution or body which is the subject of the proceedings conducted by the Supervisor the opportunity of being heard on the matters to which the Supervisor has taken objection. The European Data Protection Supervisor shall base its decisions only on objections on which the parties concerned have been able to comment. Complainants shall be associated closely with the proceedings.	
6.  The rights of defence of the parties concerned shall be fully respected in the proceedings. They shall be entitled to have access to the European Data Protection Supervisor's file, subject to the legitimate interest of individuals or undertakings in the protection of their personal data or business secrets.	6.  The rights of defence of the parties concerned shall be fully respected in the proceedings. They shall be entitled to have access to the European Data Protection Supervisor's file, subject to the legitimate interest of individuals or undertakings in the protection of their personal data or business secrets.	6.  The rights of defence of the parties concerned shall be fully respected in the proceedings. They shall be entitled to have access to the European Data Protection Supervisor's file, subject to the legitimate interest of individuals or undertakings in the protection of their personal data or business secrets.	
7.  Funds collected by imposition of	7.  Funds collected by imposition of	7.  Funds collected by imposition of	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
finances in this Article shall be the income of the general budget of the European Union.	finances in this Article shall be the income of the general budget of the European Union.	finances in this Article shall be the income of the general budget of the European Union.	
<i>Article 67</i>	<i>Article 67</i>	<i>Article 67</i>	
<i>Representation of data subjects</i>	<i>Representation of data subjects</i>	<i>Representation of data subjects</i>	
The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with Union law or the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint with the European Data Protection Supervisor on his or her behalf, to exercise the rights referred to in Articles 63 on his or her behalf, and to exercise the right to receive compensation referred to in Article 65 on his or her behalf.	The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with Union law or the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint with the European Data Protection Supervisor on his or her behalf, to exercise the rights referred to in Articles 63 on his or her behalf, and to exercise the right to receive compensation referred to in Article 65 on his or her behalf.	The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with Union law or the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint with the European Data Protection Supervisor on his or her behalf, to exercise the rights referred to in Articles 63 <b>and 64</b> on his or her behalf, and to exercise the right to receive compensation referred to in Article 65 on his or her behalf.	The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with Union law or the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint with the European Data Protection Supervisor on his or her behalf, to exercise the rights referred to in Articles 63 and 64 on his or her behalf, and to exercise the right to receive compensation referred to in Article 65 on his or her behalf.

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<i>Article 68</i>	<i>Article 68</i>	<i>Article 68</i>	
<i>Complaints by Union staff</i>	<i>Complaints by Union staff</i>	<i>Complaints by Union staff</i>	
Any person employed by a Union institution or body may lodge a complaint with the European Data Protection Supervisor regarding an alleged infringement of the provisions of this Regulation, without acting through official channels. No one shall suffer prejudice on account of a complaint lodged with the European Data Protection Supervisor alleging such an infringement.	Any person employed by a Union institution or body may lodge a complaint with the European Data Protection Supervisor regarding an alleged infringement of the provisions of this Regulation, without acting through official channels. No one shall suffer prejudice on account of a complaint lodged with the European Data Protection Supervisor alleging such an infringement.	Any person employed by a Union institution or body may lodge a complaint with the European Data Protection Supervisor regarding an alleged infringement of the provisions of this Regulation, without acting through official channels. No one shall suffer prejudice on account of a complaint lodged with the European Data Protection Supervisor alleging such an infringement.	



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<i>Article 69</i>	<i>Article 69</i>	<i>Article 69</i>	
<i>Sanctions</i>	<i>Sanctions</i>	<i>Sanctions</i>	
Any failure to comply with the obligations laid down in this Regulation, whether intentionally or through negligence on his or her part, shall make an official or other servant of the European Union liable to disciplinary or any other action, in accordance with the rules and procedures laid down in the Staff Regulations of Officials of the European Union or in the Conditions of Employment of Other Servants of the European Union.	Any failure to comply with the obligations laid down in this Regulation, whether intentionally or through negligence on his or her part, shall make an official or other servant of the European Union liable to disciplinary or any other action, in accordance with the rules and procedures laid down in the Staff Regulations of Officials of the European Union or in the Conditions of Employment of Other Servants of the European Union.	Any failure to comply with the obligations laid down in this Regulation, whether intentionally or through negligence on his or her part, shall make an official or other servant of the European Union liable to disciplinary or any other action, in accordance with the rules and procedures laid down in the Staff Regulations of Officials of the European Union or in the Conditions of Employment of Other Servants of the European Union.	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<b>AM 87</b>  <b>CHAPTER VIIIa</b>  <b>PROCESSING OF</b> <b>OPERATIONAL PERSONAL</b> <b>DATA</b>		<b>CHAPTER VIIIa</b>  <i>PROCESSING OF</i> <i>OPERATIONAL PERSONAL</i> <i>DATA BY UNION BODIES,</i> <i>OFFICES OR AGENCIES</i> <i>CARRYING OUT ACTIVITIES</i> <i>WHICH FALL WITHIN THE</i> <i>SCOPE OF CHAPTER 4 OR</i> <i>CHAPTER 5 OF TITLE V OF</i> <i>PART THREE OF THE TFEU</i>
	<b>AM 88</b>  <i>Article 69a</i>		<i>Article 69a</i>
	<i>Scope</i>		<i>Scope of the Chapter</i>
	<i>By way of derogation from Articles 4, 5, 6, 7, 8, 10, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 41, 43, 49, 50 and 51, the provisions of this Chapter shall apply to processing of operational data by Union agencies established on the basis of Chapters 4 and 5 of Title V of Part Three TFEU and by missions referred to in Article 42(1) and Articles 43 and 44 TEU.</i>		This Chapter shall apply only to the processing of operational personal data by Union bodies, offices or agencies when carrying out activities which fall within the scope of Chapter 4 and 5 of Title V of Part Three of the TFEU, without prejudice to specific data protection rules applicable to those Union bodies, offices or agencies.
	<i>Provisions relating to specific</i>		deletion

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>processing of operational personal data contained in the founding acts of these agencies may particularise and complement the application of this Regulation.</i>		
	AM 89  <i>Article 69b</i>		<i>Article 69b</i>
	<i>Principles relating to processing of operational personal data</i>		<i>Principles relating to processing of operational personal data</i>
	<i>1. Operational personal data shall be:</i>		1. Operational personal data shall be:
	<i>(a) processed lawfully and fairly ('lawfulness and fairness');</i>		(a)processed lawfully and fairly ('lawfulness and fairness');
	<i>(b) collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be</i>		(b)collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes ('purpose limitation');

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>(c) adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');</i>		c) adequate, relevant, and not excessive in relation to the purposes for which they are processed ('data minimisation');
	<i>(d) accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that operational personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');</i>		d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that operational personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ("accuracy");
	<i>(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the operational personal data are processed;</i>		e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation');
	<i>(f) processed in a manner that ensures appropriate security of the operational personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or</i>		(f) processed in a manner that ensures appropriate security of the operational personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>organisational measures ('integrity and confidentiality').</i>		organisational measures ('integrity and confidentiality').
	<i>2. Union agencies or missions shall make publicly available a document setting out in an intelligible form the provisions regarding the processing of operational personal data and the means available for the exercise of the rights of data subjects.</i>		deletion
			2. Processing by the same or another controller for any of the purposes set out in the founding act of the Union institution or body other than that for which the personal data are collected shall be permitted in so far as:
			(a) the controller is authorised to process such personal data for such a purpose in accordance with Union law; and
			(b) processing is necessary and proportionate to that other purpose in accordance with Union law.
			3. Processing by the same or another controller may include archiving in the public interest, scientific, statistical or historical

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			use, for the purposes set out in the founding act of the Union institution or body, subject to appropriate safeguards for the rights and freedoms of data subjects.
			4.The controller shall be responsible for, and be able to demonstrate compliance with, paragraphs 1, 2 and 3.
	AM 90  <i>Article 69c</i>		<i>Article 69c</i>
	<i>Lawfulness of processing</i>		<i>Lawfulness of processing of operational personal data</i>
	<i>Processing shall be lawful only if and to the extent that processing is necessary for the performance of a task carried out by Union agencies and missions and that it is based on Union law. Union law specifying and complementing this Regulation as regards the processing within the scope of this Chapter shall specify the objectives</i>		1. Processing of operational personal data shall be lawful only if and to the extent that processing is necessary for the performance of a task carried out by Union institutions and bodies when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part three of the TFEU and that it is based

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>of processing, the operational personal data to be processed and the purposes of the processing.</i>		on Union law.
			2. Specific Union legal acts regulating processing within the scope of this Chapter shall specify at least the objectives of processing, the operational personal data to be processed, the purposes of the processing and the time limits for storage of the operational personal data or for periodic review of the need for further storage of the operational personal data.
	AM 91 <i>Article 69d</i>		<i>Article 69d</i>
	<i>Distinction between different categories of data subjects</i>		<i>Distinction between different categories of data subjects</i>
	<i>Union agencies or missions shall make a clear distinction between operational personal data of different categories of data subjects, such as:</i>		The controller shall, where applicable and as far as possible, make a clear distinction between operational personal data of different categories of data subjects, such as the categories listed in the founding acts of Union institutions and bodies.

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>(a) persons who are suspected of having committed or having taken part in a criminal offence in respect of which the Union agencies or missions are competent, or who have been convicted of such an offence;</i>		deletion
	<i>(b) persons regarding whom there are factual indications or reasonable grounds to believe that they will commit criminal offences in respect of which Union agencies or missions are competent;</i>		deletion
	<i>(c) persons who have been the victims of one of the offences under consideration</i>		deletion
	<i>(d) persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings;</i>		deletion
	<i>(e) persons who can provide information on criminal offences; and</i>		deletion
	<i>(f) contacts or associates of one of the persons referred to in points (a) and (b).</i>		deletion
	AM 92 <i>Article 69e</i>		<i>Article 69e</i>



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>Distinction between operational personal data and verification of quality of operational personal data</i>		<i>Distinction between operational personal data and verification of quality of operational personal data</i>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>Union agencies and missions shall distinguish operational personal data based on facts from operational personal data based on personal assessments.</i>		1. The controller shall distinguish, as far as possible, operational personal data based on facts from operational personal data based on personal assessments.
	<i>Union agencies and missions shall process operational personal data in such a way that, where applicable, it can be established which authority provided the data or where the data has been retrieved from. Union agencies and missions shall ensure that operational personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. To that end, Union agencies and missions shall verify the quality of operational personal data before they are transmitted or made available. As far as possible, in all transmissions of operational personal data, Union agencies and missions shall add necessary information enabling the recipient to assess the degree of accuracy, completeness and reliability of</i>		2. The controller shall take all reasonable steps to ensure that operational personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. To that end, the controller shall, as far as practicable and where relevant, verify, for example by consulting with the competent authority the data originates from, the quality of operational personal data before they are transmitted or made available. As far as possible, in all transmissions of operational personal data, the controller shall add necessary information enabling the recipient to assess the degree of accuracy, completeness and reliability of operational personal data, and the extent to which they are up to date.

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>operational personal data, and the extent to which they are up to date shall be added.</i>		
	<i>If it emerges that incorrect operational personal data have been transmitted or operational personal data have been unlawfully transmitted, the recipient shall be notified without delay. In such a case, the operational personal data shall be rectified or erased or processing shall be restricted.</i>		3. If it emerges that incorrect operational personal data have been transmitted or operational personal data have been unlawfully transmitted, the recipient shall be notified without delay. In such a case, the operational personal data shall be rectified or erased or processing shall be restricted in accordance with Article 69m.
	AM 93 <i>Article 69f</i>		<i>Article 69f</i>
	<i>Specific processing conditions</i>		<i>Specific processing conditions</i>
	<i>When Union agencies and missions provide for specific conditions for processing, they shall inform the recipient of such operational personal data of those conditions and the requirement to comply with them. Union agencies and missions shall comply with specific processing conditions for processing provided by a national authority in accordance with</i>		1. When Union law applicable to the transmitting controller provides for specific conditions for processing, the controller shall inform the recipient of such operational personal data of those conditions and the requirement to comply with them.

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>Article 9 (3) and (4) of Directive (EU) 2016/680.</i>		
			2. The controller shall comply with specific processing conditions for processing provided by the transmitting national competent authority in accordance with Article 9 (3) and (4) of the Directive (EU) 2016/680.
	<b>AM 94</b> <i>Article 69g</i>		
	<i>Transmission of operational personal data to other Union institutions and bodies</i>		deletion
	<i>Union agencies and missions shall only transmit operational personal data to other Union institutions and bodies if the data are necessary for the performance of their tasks or those of the recipient Union agencies and missions. Where operational personal data are transmitted following a request from the other Union institution or body, both the controller and the recipient shall bear the responsibility for the legitimacy of</i>		

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>this transfer. Union agencies and missions shall be required to verify the competence of the other Union institution or body and to make a provisional evaluation of the necessity for the transmission. If doubts arise as to this necessity, Union agencies and missions shall seek further information from the recipient. Other Union institutions and bodies shall ensure that the necessity for the transmission can be subsequently verified. Other Union institutions and bodies shall process the personal data only for the purposes for which they were transmitted.</i>		
	AM 95 <i>Article 69h</i>		<i>Article 69h</i>
	<i>Processing of special categories of operational personal data</i>		<i>Processing of special categories of operational personal data</i>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<p><i>Processing of operational personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, operational personal data concerning health or operational personal data concerning a natural person's sex life or sexual orientation shall be prohibited, unless it is strictly necessary and proportionate for preventing or combating crime that falls within the Union agencies' or missions' objectives and if those data supplement other personal data processed by the Union agencies and missions. The selection of a particular group of persons solely on the basis of such personal data shall be prohibited.</i></p>		<p>1. Processing of operational personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, operational personal data concerning health or concerning a natural person's sex life or sexual orientation shall be allowed only where strictly necessary for operational purposes and within the mandate of the Union institution or body and subject to appropriate safeguards for the rights and freedoms of the data subject. Discrimination of natural persons on the basis of such personal data shall be prohibited.</p>
8394/1/18 REV 1		CHS/np	341

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>The data protection officer shall be informed immediately of recourse to this Article.</i>		2. The data protection officer shall be informed without undue delay of recourse to this Article.
8394/1/18 REV 1		CHS/np	342

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<p><i>Operational personal data as referred to in subparagraph above shall not be transmitted to Member States, Union bodies, third countries or international organisations unless such transmission is strictly necessary and proportionate in individual cases concerning crime that falls within the Union agencies' and missions' objectives and in accordance with Chapter V.</i></p>		deletion
8394/1/18 REV 1		CHS/np	343



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	AM 96 <i>Article 69i</i>		<i>Article 69i</i>
	<i>Automated individual decision-making, including profiling</i>		<i>Automated individual decision-making, including profiling</i>
	<i>The data subject shall have the right not to be subject to a decision of Union agencies and missions based solely on automated processing, including profiling, which produces adverse legal effects concerning him or her or similarly significantly affects him or her.</i>		Council suggestion:  1. A decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her shall be prohibited unless authorised by Union law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller.
			Council suggestion:  2. Decisions referred to in paragraph 1 of this Article shall not be based on special categories of personal data referred to in

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			Article 69h, unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.
			Council suggestion:  3. Profiling that results in discrimination against natural persons on the basis of special categories of personal data referred to in Article 69h shall be prohibited, in accordance with Union law.
			<i>Article 69ia</i>
			<i>Communication and modalities for exercising the rights of the data subject</i>
			1. The controller shall take reasonable steps to provide any information referred to in Article 69j and make any communication with regard to Articles 69k to 69n and 69od relating to processing to the data subject in a concise, intelligible and easily accessible

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			form, using clear and plain language. The information shall be provided by any appropriate means, including by electronic means. As a general rule, the controller shall provide the information in the same form as the request.
			2. The controller shall facilitate the exercise of the rights of the data subject under Articles 69j to 69n.
			3. The controller shall inform the data subject in writing about the follow up to his or her request without undue delay and in any case at the latest after three months after receipt of the request by the data subject.
			4. The controller shall provide the information under Article 69j and any communication made or action taken pursuant to Articles 69k to 69n and 69od free of

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request
			5. Where the controller has reasonable doubts concerning the identity of the natural person making a request referred to in Article 69k or 69m, the controller may request the provision of additional information necessary to confirm the identity of the data subject.
	AM 97 <i>Article 69j</i>		<i>Article 69j</i>
	<i>Information to be made available or given to the data subject</i>		<i>Information to be made available or given to the data subject</i>
	<i>1. Union agencies and missions shall make available to the data subject at least the following</i>		1. The controller shall make available to the data subject at

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>information:</i>		least the following information:
	<i>(a) the identity and the contact details of the Union agency or mission;</i>		(a) the identity and the contact details of the Union institution or body
	<i>(b) the contact details of the data protection officer;</i>		(b) the contact details of the data protection officer
	<i>(c) the purposes of the processing for which the operational personal data are intended;</i>		(c) the purposes of the processing for which the operational personal data are intended;
	<i>(d) the right to lodge a complaint with the European Data Protection Supervisor and its contact details;</i>		(d) the right to lodge a complaint with the European Data Protection Supervisor and its contact details;
	<i>(e) the existence of the right to request from Union agencies and missions access to and rectification or erasure of operational personal data and restriction of processing of the operational personal data concerning the data subject.</i>		(e) the existence of the right to request from the controller access to and rectification or erasure of operational personal data and restriction of processing of the operational personal data concerning the data subject.
	<i>2. In addition to the information referred to in paragraph 1, Union agencies and missions shall give to the data subject, in specific cases, the following further information to enable the exercise of his or her</i>		2. In addition to the information referred to in paragraph 1, the controller shall give to the data subject, in specific cases foreseen in Union law, the following further information to enable the

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>rights;</i>		exercise of his or her rights;
	<i>(a) the legal basis for the processing;</i>		(a) the legal basis for the processing;
	<i>(b) the period for which the operational personal data will be stored, or, where that is not possible, the criteria used to determine that period;</i>		(b) the period for which the operational personal data will be stored, or, where that is not possible, the criteria used to determine that period;
	<i>(c) the categories of recipients of the operational personal data, including in third countries or international organisations;</i>		(c) where applicable, the categories of recipients of the operational personal data, including in third countries or international organisations;
	<i>(d) where necessary, further information, in particular where the operational personal data are collected without the knowledge of the data subject.</i>		d) where necessary, further information, in particular where the operational personal data are collected without the knowledge of the data subject.
	<i>3. Union agencies and missions may delay, restrict or omit the provision of the information to the data subject pursuant to paragraph 2 to the extent that, and for as long as, such a measure is provided for by a legal act adopted on the basis of the Treaties and constitutes a</i>		3. The controller may delay, restrict or omit the provision of the information to the data subject pursuant to paragraph 2 to the extent that, and for as long as, such a measure constitutes a necessary and proportionate

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, in order to:</i>		measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, in order to:
	<i>(a) avoid obstructing official or legal inquiries, investigations or procedures;</i>		(a) avoid obstructing official or legal inquiries, investigations or procedures;
	<i>(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;</i>		(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
	<i>(c) protect public security of the Member States;</i>		(c) protect public security of the Member States;
	<i>(d) protect national security of the Member States;</i>		(d) protect national security of the Member States;
	<i>(e) protect the rights and freedoms of others.</i>		(e) protect the rights and freedoms of others.
	AM 98 <i>Article 69k</i>		<i>Article 69k</i>
	<i>Right of access by the data subject</i>		<i>Right of access by the data subject</i>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>Any data subject shall have the right to obtain from Union agencies and missions confirmation as to whether or not operational personal data concerning him or her are processed, and be given access to the following information:</i>		The data subject shall have the right to obtain from the controller confirmation as to whether or not operational personal data concerning him or her are processed, and where that is the case, have the right to access operational personal data and the following information:
	<i>(a) the purposes of and legal basis of the processing operation;</i>		a) the purposes of and legal basis for the processing
	<i>(b) the categories of operational personal data concerned;</i>		(b) the categories of operational personal data concerned;
	<i>(c) the recipients or categories of recipients to whom the operational personal data have been disclosed, in particular recipients in third countries or international organisations;</i>		c) the recipients or categories of recipients to whom the operational personal data have been disclosed, in particular recipients in third countries or international organisations;
	<i>(d) the envisaged period for which the operational personal data will be stored;</i>		d) where possible, the envisaged period for which the operational personal data will be stored, or, if not possible, the criteria used to determine that period;
	<i>(e) the existence of the right to</i>		(e) the existence of the right to



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>request from Union agencies and missions rectification or erasure of operational personal data or restriction of processing of operational personal data concerning the data subject;</i>		request from the controller rectification or erasure of operational personal data or restriction of processing of operational personal data concerning the data subject;
	<i>(f) the right to lodge a complaint with the European Data Protection Supervisor and his or her contact details;</i>		(f) the right to lodge a complaint with the European Data Protection Supervisor and his or her contact details;

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>(g) communication of the operational personal data undergoing processing and of any available information as to their sources.</i>		(g) communication of the operational personal data undergoing processing and of any available information as to their origin.
	AM 99 <i>Article 69I</i>		<i>Article 69I</i>
	<i>Limitations to the right of access</i>		<i>Limitations to the right of access</i>
	<i>1. Union agencies and missions may restrict, wholly or partly, the data subject's right of access to the extent that, and for as long as, such a partial or complete restriction is provided for by a legal act adopted on the basis of the Treaties and constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned, in order to:</i>		1. The controller may restrict, wholly or partly, the data subject's right of access to the extent that, and for as long as, such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned, in order to:
	<i>(a) avoid obstructing official or legal inquiries, investigations or procedures;</i>		(a) avoid obstructing official or legal inquiries, investigations or procedures;

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;</i>		(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
	<i>(c) protect public security of the Member States;</i>		(c) protect public security of the Member States;
	<i>(d) protect national security of the Member States;</i>		(d) protect national security of the Member States;
	<i>(f) protect the rights and freedoms of others.</i>		(e) protect the rights and freedoms of others, such as victims and witnesses.
	<i>2. In the cases referred to in paragraph 1, Union agencies and missions shall inform the data subject, without undue delay, in writing of any refusal or restriction of access and of the reasons for the refusal or the restriction. Such information may be omitted where its provision would undermine a purpose under paragraph 1. Union agencies and missions shall inform the data subject of the possibility of</i>		2. In the cases referred to in paragraph 1, the controller shall inform the data subject, without undue delay, in writing of any refusal or restriction of access and of the reasons for the refusal or the restriction. Such information may be omitted where its provision would undermine a purpose under paragraph 1. The controller shall inform the data subject of the possibility of

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>lodging a complaint with the European Data Protection Supervisor or of seeking a judicial remedy in the Court of Justice of the European Union. Union agencies and missions shall document the factual or legal reasons on which the decision is based. That information shall be made available to the European Data Protection Supervisor on request.</i>		lodging a complaint with the European Data Protection Supervisor or of seeking a judicial remedy in the Court of Justice of the European Union. The controller shall document the factual or legal reasons on which the decision is based. That information shall be made available to the European Data Protection Supervisor on request.
	AM 100 <i>Article 69m</i>		<i>Article 69m</i>
	<i>Right to rectification or erasure of operational personal data and restriction of processing</i>		<i>Right to rectification or erasure of operational personal data and restriction of processing</i>
	<i>1. Any data subject shall have the right to obtain from Union agencies and missions without undue delay the rectification of inaccurate operational personal data relating to him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete operational personal data completed, including by means of providing a supplementary</i>		1. Any data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate operational personal data relating to him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete operational personal data completed, including by means of providing a supplementary statement.

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>statement.</i>		
	<i>Union agencies and missions shall erase operational personal data without undue delay and the data subject shall have the right to obtain from Union agencies and missions the erasure of operational personal data concerning him or her without undue delay where processing infringes Articles 69b, 69c or 69h, or where operational personal data must be erased in order to comply with a legal obligation to which Union agencies and missions are subject.</i>		2. The controller shall erase operational personal data without undue delay and the data subject shall have the right to obtain from the controller the erasure of operational personal data concerning him or her without undue delay where processing infringes Articles 69b, 69c (1) or 69h, or where operational personal data must be erased in order to comply with a legal obligation to which the controller is subject.
	(EP to check erratum missing end of paragraph 1 “Instead of erasure, Union agencies and missions shall restrict processing where:”)		3. Instead of erasure, the controller shall restrict processing where:
	<i>(a) the accuracy of the personal data is contested by the data subject and their accuracy or inaccuracy cannot be ascertained; or</i>		(a) the accuracy of the personal data is contested by the data subject and their accuracy or inaccuracy cannot be ascertained;

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			or
	<i>(b) the personal data must be maintained for the purposes of evidence.</i>		(b) the personal data must be maintained for the purposes of evidence.
	<i>2. Where processing is restricted pursuant to point (a) of the first subparagraph, Union agencies and missions shall inform the data subject before lifting the restriction of processing. Restricted data shall be processed only for the purpose that prevented their erasure.</i>		Where processing is restricted pursuant to point (a) of the first subparagraph, the controller shall inform the data subject before lifting the restriction of processing.  Restricted data shall be processed only for the purpose that prevented their erasure.
	<i>3. Union agencies and missions shall inform the data subject in writing of any refusal of rectification or erasure of operational personal data or restrict processing and of the reasons for the refusal. Union agencies and missions may restrict, wholly or partly, the obligation to provide such information to the extent that such a restriction constitutes a necessary and proportionate measure in a democratic society with due regard</i>		4. The controller shall inform the data subject in writing of any refusal of rectification or erasure of operational personal data or restrict processing and of the reasons for the refusal. The controller may restrict, wholly or partly, the obligation to provide such information to the extent that such a restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>for the fundamental rights and legitimate interests of the natural person concerned in order to:</i>		fundamental rights and legitimate interests of the natural person concerned in order to:
	<i>(a) avoid obstructing official or legal inquiries, investigations or procedures;</i>		(a) avoid obstructing official or legal inquiries, investigations or procedures;
	<i>(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;</i>		(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
	<i>(c) protect public security of the Member States;</i>		(c) protect public security of the Member States;
	<i>(d) protect national security of the Member States;</i>		(d) protect national security of the Member States;
	<i>(f) protect the rights and freedoms of others.</i>		(e) protect the rights and freedoms of others.
	<i>4. Union agencies and missions shall inform the data subject of the possibility of lodging a complaint with the European Data Protection Supervisor or seeking a judicial</i>		The controller shall inform the data subject of the possibility of lodging a complaint with the European Data Protection Supervisor or seeking a judicial

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>remedy from the Court of Justice of the European Union.</i>		remedy from the Court of Justice of the European Union.
	<i>5. Union agencies and missions shall communicate the rectification of inaccurate personal data to the competent authority from which the inaccurate operational personal data originate.</i>		5. The controller shall communicate the rectification of inaccurate personal data to the competent authority from which the inaccurate operational personal data originate
	<i>6. Union agencies and missions shall, where operational personal data has been rectified or erased or processing has been restricted pursuant to paragraphs 1, 2 and 3, notify the recipients and inform them that they have to rectify or erase the operational personal data or restrict processing of the operational personal data under their responsibility.</i>		6. The controller shall, where operational personal data has been rectified or erased or processing has been restricted pursuant to paragraphs 1, 2 and 3, notify the recipients and inform them that they have to rectify or erase the operational personal data or restrict processing of the operational personal data under their responsibility.
			<p><i>Article 69ma</i></p> <p><i>Right of access in criminal investigations and proceedings</i></p> <p>Where operational personal data originates from a national competent authority, Union agencies, offices and bodies shall,</p>



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			prior to a decision on the data subject right of access, verify with the concerned competent authority whether such personal data are contained in a judicial decision or record or a case file processed in the course of criminal investigations and proceedings in the Member State of that competent authority. Where this is the case, a decision on the right of access shall be taken in consultation and close cooperation with the concerned competent authority.
	<b>AM 101</b> <i>Article 69n</i>		<i>Article 69n</i>
	<i>Exercise of rights by the data subject and verification by the European Data Protection Supervisor</i>		<i>Exercise of rights by the data subject and verification by the European Data Protection Supervisor</i>
	<i>In the cases referred to in Articles 69j(3), 69k and 69m(4), the rights of the data subject may also be exercised through the European Data Protection Supervisor.</i>		1. In the cases referred to in Articles 69j(3), 69l and 69m(4), the rights of the data subject may also be exercised through the European Data Protection Supervisor.

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>Union agencies and missions shall inform the data subject of the possibility of exercising his or her rights through the European Data Protection Supervisor pursuant to paragraph 1.</i>		2. The controller shall inform the data subject of the possibility of exercising his or her rights through the European Data Protection Supervisor pursuant to paragraph 1
	<i>Where the right referred to in paragraph 1 is exercised, the European Data Protection Supervisor shall at least inform the data subject that all necessary verifications or a review by it have taken place. The European Data Protection Supervisor shall also inform the data subject of his or her right to seek a judicial remedy in the Court of Justice of the European Union.</i>		3. Where the right referred to in paragraph 1 is exercised, the European Data Protection Supervisor shall at least inform the data subject that all necessary verifications or a review by it have taken place. The European Data Protection Supervisor shall also inform the data subject of his or her right to seek a judicial remedy in the Court of Justice of the European Union.
			<i>Article 69na</i>
			<i>Data protection by design and by default</i>
			1. The controller shall, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing, as well as

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing, in order to meet the requirements of this Regulation and its founding act, and protect the rights of the data subjects.
			2. The controller shall implement appropriate technical and organisational measures ensuring that, by default, only operational personal data which are adequate, relevant and not excessive in relation to the purpose of the processing are processed. That obligation applies to the amount of operational personal data

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default operational personal data are not made accessible without the individual's intervention to an indefinite number of natural persons
			<i>Article 69nb</i>
			<i>Joint controllers</i>
			1. Where a controller, jointly with one or more controllers or controllers other than Union institutions and bodies, determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with their data protection obligations, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Article 69j, by

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			means of an arrangement between them unless, and in so far as, the respective responsibilities of the joint controllers are determined by Union or Member State law to which the joint controllers are subject. The arrangement may designate a contact point for data subjects.
			2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.
			3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.
			<i>Article 69nc</i>
			<i>Processor</i>
			1. Where processing is to be

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and the founding act of the controller and ensure the protection of the rights of the data subject
			2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.
			3. Processing by a processor shall be governed by a contract or other legal act under Union law, or the law of a Member State of the

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			European Union, that is binding on the processor with regard to the controller and that sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of operational personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:
			(a) acts only on instructions from the controller;
			(b) ensures that persons authorised to process the operational personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
			(c) assists the controller by any appropriate means to ensure compliance with the provisions on the data subject's rights;
			(d) at the choice of the controller, deletes or returns all the operational personal data to the controller after

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			the end of the provision of services relating to processing, and deletes existing copies unless Union law or the law of a Member State of the European Union requires storage of the operational personal data;
			(e) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article;
			(f) complies with the conditions referred to in paragraphs 2 and 3 for engaging another processor.
			4.The contract or the other legal act referred to in paragraphs 3 shall be in writing, including in electronic form.
			5. If a processor infringes this Regulation or the founding act of the controller by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.
	<b>AM 102</b> <i>Article 69o</i>		<i>Article 69o</i>



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>Logging</i>		<i>Logging</i>
	<i>Union agencies and missions shall keep logs for any of the following processing operations in automated processing systems: the collection, alteration, access, consultation, disclosure, including transfers, combination and erasure of operational personal data.</i>		1. The controller shall keep logs for any of the following processing operations in automated processing systems: the collection, alteration, access, consultation, disclosure, including transfers, combination and erasure of operational personal data. The logs of consultation and disclosure shall make it possible to establish the justification for, and the date and time of, such operations, the identification of the person who consulted or disclosed operational personal data, and, as far as possible, the identity of the recipients of such operational personal data.
	<i>The logs of consultation and disclosure shall make it possible to establish the justification for, and the date and time of, such operations, the identification of the person who consulted or disclosed operational personal data, and, as far as possible, the identity of the recipients of such operational personal data. Such logs shall only be used for the</i>		2. The logs shall be used solely for verification of the lawfulness of processing, self-monitoring, ensuring the integrity and security of the operational personal data, and for criminal proceedings. Such logs shall be deleted after three years, unless they are required for on-going control.

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>control of data protection and for ensuring proper data processing as well as data integrity and security. It shall not be possible to modifying such logs. Such logs shall be deleted after three years, unless they are required for on-going control.</i>		
	<i>Union agencies or missions shall make the logs available to the European Data Protection Supervisor and their respective data protection officers on request.</i>		3. The controller shall make the logs available to the European Data Protection Supervisor and their respective data protection officers on request
			<i>Article 69oa</i>
			<i>Data protection impact assessment</i>
			1. Where a type of processing, in particular, using new technologies, and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall carry out, prior to the processing, an assessment of the impact of the envisaged processing operations on the protection of

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			operational personal data.
			2. The assessment referred to in paragraph 1 shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address those risks, safeguards, security measures and mechanisms to ensure the protection of operational personal data and to demonstrate compliance with data protection rules, taking into account the rights and legitimate interests of the data subjects and other persons concerned.
			<i>Article 69ob</i>
			<i>Prior consultation of the European Data Protection Supervisor</i>
			1. The controller shall consult the European Data Protection Supervisor prior to processing which will form part of a new filing system to be created, where
			(a) a data protection impact

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			assessment as provided for in Article 69oa indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk; or
			b) the type of processing, in particular, where using new technologies, mechanisms or procedures, involves a high risk to the rights and freedoms of data subjects.
			2. The European Data Protection Supervisor may establish a list of the processing operations which are subject to prior consultation pursuant to paragraph 1.
			3. The controller shall provide the European Data Protection Supervisor with the data protection impact assessment pursuant to Article 69oa and, on request, with any other information to allow the European Data Protection Supervisor to make an assessment of the compliance of the processing and

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			in particular of the risks for the protection of operational personal data of the data subject and of the related safeguards.
			<p>Council suggestion:</p> <p>4. Where the European Data Protection Supervisor is of the opinion that the intended processing referred to in paragraph 1 of this Article would infringe this Regulation or the founding legal act of the controller, in particular where the controller has insufficiently identified or mitigated the risk, the European Data Protection Supervisor shall provide, within a period of up to six weeks of receipt of the request for consultation, written advice to the controller. That period may be extended by a month, taking into account the complexity of the intended processing. The European Data Protection Supervisor shall inform the controller of any such extension within one month of receipt of the</p>

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			request for consultation, together with the reasons for the delay.
			<i>Article 69oc</i>
			<i>Notification of a personal data breach to the European Data Protection Supervisor</i>
			1. In the case of a personal data breach, the controller shall notify without undue delay and, where feasible, not later than 72 hours after having become aware of it, the personal data breach to the European Data Protection Supervisor, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the European Data Protection Supervisor is not made within 72 hours, it shall be accompanied by reasons for the delay.
			2. The notification referred to in paragraph 1 shall at least:
			a) describe the nature of the

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
			(b) communicate the name and contact details of the Data Protection Officer;
			(c) describe the likely consequences of the personal data breach;
			(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
			3. Where, and in so far as, it is not possible to provide the information referred to in paragraph 2 at the same time, the information may be provided in

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			phases without undue further delay.
			4. The controller shall document any personal data breaches referred to in paragraph 1, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the European Data Protection Supervisor to verify compliance with this Article
			5. Where the personal data breach involves personal data that have been transmitted by or to the competent authorities, the controller shall communicate the information referred to in paragraph 2 to the competent authorities of the Member States concerned without undue delay.
			<i>Article 69od</i>
			<i>Communication of a personal data breach to the data subject</i>
			1. Where the personal data breach



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.
			2. The communication to the data subject referred to in paragraph 1 of this Article shall describe, in clear and plain language the nature of the personal data breach and shall contain at least the information and the recommendations provided for in points (b), (c) and (d) of Article 69oc(2).
			3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:
			(a) the controller has implemented appropriate technological and organisational protection measures, and that those measures were applied to the personal data affected by the personal data breach, in particular those that

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
			(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
			(c) it would involve a disproportionate effort. In such a case, there shall instead be a public communication or a similar measure whereby the data subjects are informed in an equally effective manner.
			4. If the controller has not already communicated the personal data breach to the data subject, the European Data Protection Supervisor, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so, or may decide that any of the conditions referred to in paragraph 3 are met.

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			5. The communication to the data subject referred to in paragraph 1 of this Article may be delayed, restricted or omitted subject to the conditions and on the grounds referred to in Article 69j(3).
			<i>Article 69oe</i>
			<i>Security of processing of operational personal data</i>
			1. The controller and the processor shall, taking into account the state of the art, costs of implementation and the nature, scope, context and purposes of the processing as well as risk of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in particular as regards the processing of special categories of operational personal data.
			2. In respect of automated processing, the controller and the processor shall, following an

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			evaluation of the risks, implement measures designed to
			(a) deny unauthorised persons access to data processing equipment used for processing (equipment access control);
			(b) prevent the unauthorised reading, copying, modification or removal of data media (data media control);
			(c) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data (storage control);
			(d) prevent the use of automated processing systems by unauthorised persons using data communication equipment (user control);
			(e) ensure that persons authorised to use an automated processing system have access only to the personal data covered by their access authorisation (data access

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			control);
			(f) ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication (communication control);
			(g) ensure that it is subsequently possible to verify and establish which personal data have been input into automated data processing systems, and when and by whom the data were input (input control);
			(h) prevent unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media (transport control);
			(i) ensure that installed systems may, in the case of interruption, be restored (recovery);
			(j) ensure that the functions of the

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			system perform, that the appearance of faults in the functions is reported (reliability) and that stored personal data cannot be corrupted by means of a malfunctioning of the system (integrity).
	AM 103 <i>Article 69p</i>		<i>Article 69p</i>
	<i>Transfer of operational personal data to third countries and international organisations</i>		<i>Transfer of operational personal data to third countries and international organisations</i>
	<i>1 Subject to any possible restrictions pursuant to Article 69l, Union agencies or missions may transfer operational personal data to an authority of a third country or to an international organisation insofar as such transfer is necessary for the performance of the tasks of the Union agencies or missions, on the basis of one of the following:</i>		1. Subject to restrictions and conditions laid down in the founding acts of the Union institution or body, the controller may transfer operational personal data to an authority of a third country or to an international organisation insofar as such transfer is necessary for the performance of controller's tasks and only where the conditions laid down in this Article are met, namely:
	<i>(a) a decision of the Commission adopted in accordance with Article 36 of Directive (EU) 2016/680,</i>		(a) the Commission has adopted a decision in accordance with

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>finding that the third country or a territory or a processing sector within that third country or the international organisation in question ensures an adequate level of protection ('adequacy decision');</i>		Article 36 of Directive (EU) 2016/680, finding that the third country or a territory or a processing sector within that third country or the international organisation in question ensures an adequate level of protection ('adequacy decision');
	<i>(b) an international agreement concluded between the Union and that third country or international organisation pursuant to Article 218 TFEU adducing adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals;</i>		(b) in the absence of the Commission adequacy decision, an international agreement has been concluded between the Union and that third country or international organisation pursuant to Article 218 TFEU adducing adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals; an international agreement has been concluded between the Union and that third country or international organisation pursuant to Article 218 TFEU adducing adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals;

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>(c) a cooperation agreement allowing for the exchange of operational personal data concluded, before the date of application of the respective funding legal act of the Union agencies, between Union agencies or missions and that third country or international organisation in accordance with Article 23 of Decision 2009/371/JHA. Union agencies and missions may conclude administrative arrangements to implement such agreements or adequacy decisions.</i>		(c) in the absence of the Commission adequacy decision or the international agreement referred to in point (b), a cooperation agreement has been concluded allowing for the exchange of operational personal data before the entry into application of the respective founding act of the Union institution or body, between the Union institution or body and that third country.
	<i>2. Where applicable, the Executive Director shall inform the Management Board about exchanges of operational personal data on the basis of adequacy decisions pursuant to point (a) of paragraph 1.</i>		2. The founding legal acts of Union institutions and bodies may maintain or introduce more specific provisions on the conditions for international transfers of operational personal data, in particular on the transfers by way of appropriate safeguards and derogations for specific situations.
	<i>3. Union agencies and missions shall publish on their website and keep up to date a list of adequacy decisions, agreements,</i>		2a. The controller shall publish on their website and keep up to date a list of adequacy decisions, agreements, administrative



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>administrative arrangements and other instruments relating to the transfer of operational personal data in accordance with paragraph 1.</i>		arrangements and other instruments relating to the transfer of operational personal data in accordance with paragraph 1.
	<i>4. By 14 June 2021, the Commission shall assess the provisions contained in the cooperation agreements referred to in point (c) of paragraph 1, in particular those concerning data protection. The Commission shall inform the European Parliament and the Council about the outcome of that assessment and may, if appropriate, submit to the Council a recommendation for a decision authorising the opening of negotiations for the conclusion of an international agreement as referred to in point (b) of paragraph 1.</i>		deletion
	<i>5. By way of derogation from paragraph 1, where applicable, the Executive Director may authorise the transfer of operational personal data to third countries or international organisations on a case-by-case basis if the transfer is:</i>		deletion

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>(a) necessary in order to protect the vital interests of the data subject or of another person;</i>		
	<i>(b) necessary to safeguard the legitimate interests of the data subject where the law of the Member State transferring the personal data so provides;</i>		
	<i>(c) essential for the prevention of an immediate and serious threat to the public security of a Member State or a third country;</i>		
	<i>(d) necessary in individual cases for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal sanctions; or</i>		
	<i>(e) necessary in individual cases for the establishment, exercise or defence of legal claims relating to the prevention, investigation, detection or prosecution of a specific criminal offence or the execution of a specific criminal sanction.</i>		
	<i>Operational personal data shall not be transferred if the Executive Director determines that fundamental rights and freedoms</i>		deletion

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>of the data subject concerned override the public interest in the transfer referred to in points (d) and (e).</i>		
	<i>Derogations may not be applicable to systematic, massive or structural transfers.</i>		deletion
	<i>6. By way of derogation from paragraph 1, where applicable, the Management Board may, in agreement with the EDPS, authorise for a period not exceeding one year, which shall be renewable, a set of transfers in accordance with points (a) to (e) of paragraph 5, taking into account the existence of adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals. Such authorisation shall be duly justified and documented.</i>		deletion
	<i>7. The Executive Director shall inform the Management Board and the European Data Protection Supervisor as soon as possible of the cases in which paragraph 5 has been applied.</i>		deletion

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>8. Union agencies and missions shall keep detailed records of all transfers made pursuant to this Article.</i>		3. The controller shall keep detailed records of all transfers made pursuant to this Article.
			<p><i>Article 69q</i></p> <p><i>Supervision by the European Data Protection Supervisor</i></p> <p>Council suggestion:</p> <p>The rules of the founding acts of the Union bodies, offices or agencies carrying out the activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU may oblige the European Data Protection Supervisor, in the exercise of his or her supervision powers, to take utmost account the secrecy of judicial inquiries and criminal proceedings, in accordance with Union or Member State law.</p>
<b>CHAPTER IX IMPLEMENTING</b>	<b>CHAPTER IX IMPLEMENTING</b>	<b>CHAPTER IX IMPLEMENTING</b>	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
ACTS	ACTS	ACTS	
<i>Article 70</i>	<i>Article 70</i>	<i>Article 70</i>	
<i>Committee procedure</i>	<i>Committee procedure</i>	<i>Committee procedure</i>	
1.The Commission shall be assisted by the committee established by Article 93 of Regulation (EU) 2016/679. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.	1.The Commission shall be assisted by the committee established by Article 93 of Regulation (EU) 2016/679. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.	1.The Commission shall be assisted by the committee established by Article 93 of Regulation (EU) 2016/679. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.	
2.Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.	2.Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.	2.Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	AM 104 <i>CHAPTER IXa REVIEW</i>		<i>CHAPTER IXa REVIEW</i>
	AM 105 <i>Article 70a</i>		<i>Article 70a</i>
	<i>Review clause</i>		<i>Review clause</i>
	<i>1. No later than 1 June 2021, and every five years thereafter, the Commission shall present to the European Parliament a report on the application of this Regulation, accompanied, if necessary, by appropriate legislative proposals.</i>		1. No later than 1 June 2021, and every five years thereafter, the Commission shall present to the European Parliament and the Council a report on the application of this Regulation, accompanied, if necessary, by appropriate legislative proposals.
	<i>2. The ex-post evaluation outlined in paragraph 1 shall pay particular attention to the appropriateness of the scope of this Regulation, its consistency with other legislative acts in the field of data protection and assess, in particular, the implementation of Chapter V of this Regulation.</i>		deletion

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>3. No later than 1 June 2021, and every five years thereafter, the Commission shall report to the European Parliament on the application of Chapter VIII of this Regulation and the penalties and sanctions applied.</i>		deletion
	AM 106 <i>Article 70b</i>		Article 70b
	<i>Review of Union legal acts</i>		Review of Union legal acts
	<i>By 25 May 2021, the Commission shall review other legal acts adopted on the basis of the Treaties which regulate the processing of personal data, in particular by agencies established under Chapters 4 and 5 of Title V of Part Three TFEU, in order to assess the need to align them with this Regulation and to make, where appropriate, the necessary proposal to amend those acts in order to ensure a consistent approach to the protection of personal data within the scope of this Regulation.</i>		Council suggestion:  By 1 May 2022, the Commission shall review legal acts adopted on the basis of the Treaties which regulate the processing of operational personal data by Union bodies, offices or agencies when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU, in order to assess their consistency with Directive (EU) 2016/680 and Chapter VIIIa and to identify any divergences that may hamper the exchange of personal data between Union bodies, offices or agencies carrying out activities in those fields and

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
			<p>competent authorities in Member States and that may create legal fragmentation of the data protection legislation in the Union.</p> <p>On the basis of the review, in order to ensure uniform and consistent protection of natural persons with regard to processing, the Commission may in particular submit with a view to applying Chapter VIIIa to Europol and the European Public Prosecutor's Office, appropriate legislative proposals, including adaptations of Chapter VIIIa, if necessary.</p>



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	AM 107 <i>Article 71 a</i>		
	<i>Amendments to Regulation (EC) No 1987/2006</i>		deletion
	<i>Regulation (EC) No 1987/2006 of the European Parliament and of the Council <sup>1a</sup> is amended as follows:</i>		
	<i>Article 46 is replaced by the following:</i>		
	<i>"National supervisory authorities and the European Data Protection Supervisor shall, each acting within their respective competences, cooperate with each other in accordance with Article 62 of [New Regulation 45/2001]".</i>		
	<hr/> <i><sup>1a</sup> Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 381, 28.12.2006, p. 4).</i>		

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<b>AM 108</b> <i>Article 71 b</i>		
	<i>Amendments to Council Decision 2007/533/JHA</i>		deletion
	<i>Council Decision 007/533/JHA<sup>1a</sup> is amended as follows:</i>		
	<i>Article 62 of is replaced by the following:</i>		
	<i>"National supervisory authorities and the European Data Protection Supervisor shall, each acting within their respective competences, cooperate with each other in accordance with Article 62 of [New Regulation 45/2001]".</i>		
	<hr/> <i><sup>1a</sup> Council Decision 2007/533/JHA1b of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 205, 7.8.2007, p. 63).</i>		
	<b>AM 109</b> <i>Article 71c</i>		
	<i>Amendments to Regulation (EC) No 767/2008</i>		deletion
	<i>Regulation (EC) No 767/2008 of the European Parliament and the Council<sup>1a</sup> is amended as follows:</i>		

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>Article 43 is replaced by the following:</i>		
	<i>"National supervisory authorities and the European Data Protection Supervisor shall, each acting within their respective competences, cooperate with each other in accordance with Article 62 of [New Regulation 45/2001]".</i>		
	<hr/> <i><sup>1a</sup> Regulation (EC) No 767/2008 of the European Parliament and the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) (OJ L 218, 13.8.2008, p. 60).</i>		
	<b>AM 110</b>		
	<i>Article 71d</i>		
	<i>Amendments to Council Regulation (EC) No 515/97</i>		deletion
	<i>Council Regulation (EC) No 515/97<sup>1a</sup> is amended as follows:</i>		
	<i>In Article 37, paragraph 4 is replaced by the following:</i>		

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>"National supervisory authorities and the European Data Protection Supervisor shall, each acting within their respective competences, cooperate with each other in accordance with Article 62 of [New Regulation 45/2001]"</i> .		
	<hr/> <i><sup>1a</sup> Council Regulation (EC) No 515/97 of 13 March 1997 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters (OJ L 82, 22.3.1997, p. 1).</i>		
	AM 111 <i>Article 71e</i>		
	<i>Amendments to Council decision 2009/917/JHA</i>		deletion
	<i>Council Decision 2009/917/JHA<sup>1a</sup> is amended as follows:</i>		
	<i>(1) Article 25 is deleted.</i>		
	<i>(2) In Article 26, paragraphs 2 and 3 are replaced by the following:</i>		

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>"National supervisory authorities and the European Data Protection Supervisor shall, each acting within their respective competences, cooperate with each other in accordance with Article 62 of [New Regulation 45/2001]"</i> .		
	<hr/> <i><sup>1a</sup> Council Decision 2009/917/JHA of 30 November 2009 on the use of information technology for customs purposes (OJ L 323, 10.12.2009, p. 20).</i>		
	<b>AM 112</b> <i>Article 71f</i>		
	<i>Amendments to Regulation (EU) No 1024/2012</i>		deletion
	<i>Regulation (EU) No 1024/2012 of the European Parliament and of the Council<sup>1a</sup> is amended as follows:</i>		
	<i>In Article 21, paragraphs 3 and 4 are deleted.</i>		

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<hr/> <i><sup>1a</sup> Regulation (EU) No 1024/2012 of the European Parliament and of the Council of 25 October 2012 on administrative cooperation through the Internal Market Information System and repealing Commission Decision 2008/49/EC ('the IMI Regulation') (OJ L 316, 14.11.2012, p. 1).</i>		
	<b>AM 113</b> <i>Article 71g</i>		
	<i>Amendments to Commission Implementing Regulation (EU) 2015/2447</i>		deletion
	<i>Commission Implementing Regulation (EU) 2015/2447<sup>1a</sup> is amended as follows:</i>		
	<i>In Article 83, paragraph 8 is deleted.</i>		
	<hr/> <i><sup>1a</sup> Commission Implementing Regulation (EU) 2015/2447 of 24 November 2015 laying down detailed rules for implementing certain provisions of Regulation (EU) No 952/2013 of the European Parliament and of the Council laying down the Union Customs Code (OJ L 343, 29.12.2015, p. 558).</i>		

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	AM 114 <i>Article 71h</i>		
	<i>Amendments to Regulation (EU) 2016/794</i>		deletion
	<i>Regulation (EU) 2016/794 of the European Parliament and of the Council<sup>1a</sup> is amended as follows:</i>		
	<i>(1) Articles 25, 28, 30, 36, 37, 40, 41 and 46 are deleted.</i>		
	<i>(2) Article 44 is replaced by the following:</i>		
	<i>"National supervisory authorities and the EDPS shall, each acting within their respective competences, cooperate with each other in accordance with Article 62 of [New Regulation 45/2001]".</i>		
	<hr/> <sup>1a</sup> <i>Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 24.5.2016, p. 53).</i>		

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	AM 115 <i>Article 71 i</i>		
	<i>Amendments to Council Regulation (EU) 2017/XX</i>		deletion
	<i>Council Regulation (EU) 2017/...<sup>1a</sup> is amended as follows:</i>		
	<i>(1) Articles 36e, 36f, 37, 37b, 37c, 37cc, 37ccc, 37d, 37e, 37f, 37g, 37h, 37i, 37j, 37k, 37n, 37o, 41, 41a, 41b, 43a, 43b, 43c, 43d, 43e and 46 are deleted.</i>		
	<i>(2) Article 45 is replaced by the following:</i>		
	<i>"National supervisory authorities and the European Data Protection Supervisor shall, each acting within their respective competences, cooperate with each other in accordance with Article 62 of [New Regulation 45/2001]".</i>		
	<hr/> <i><sup>1a</sup> Council Regulation (EU) 2017/... of ... of implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ("the EPPO") (OJ L ...).</i>		



COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	AM 116 <i>Article 71 j</i>		
	<i>Amendments to Regulation (EU) 2017/XX</i>		
	<i>Regulation (EU) 2017/... of the European Parliament and of the Council<sup>1a</sup> is amended as follows:</i>		deletion
	<i>(1) Articles 27, 29, 30, 31, 33, 36 and 37 are deleted.</i>		
	<i>(2) Article 35 is replaced by the following:</i>		
	<i>"National supervisory authorities and the European Data Protection Supervisor shall, each acting within their respective competences, cooperate with each other in accordance with Article 62 of [New Regulation 45/2001]".</i>		
	<hr/> <i><sup>1a</sup> Regulation (EU) 2017/... of the European Parliament and of the Council on the European Union Agency for Criminal Justice Cooperation (Eurojust) (OJ L ...).</i>		

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<i>AM 117</i> <i>Article 71 k</i>		
	<i>Amendments to Eurodac Regulation (EU) 2017/XX</i>		deletion
	<i>Regulation (EU) 2017/... of the European Parliament and of the Council<sup>1a</sup> is amended as follows:</i>		
	<i>(1) Articles 29, 30, 31, and 39 are deleted.</i>		
	<i>(2) Article 34 is replaced by the following:</i>		
	<i>"National supervisory authorities and the European Data Protection Supervisor shall, each acting within their respective competences, cooperate with each other in accordance with Article 62 of [New Regulation 45/2001]".</i>		

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
	<hr/> <p><i>1<sup>a</sup> Regulation (EU) 2017/... of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (OJ L ...)</i></p>		

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<b>CHAPTER X</b> <b>FINAL PROVISIONS</b>	<b>CHAPTER X</b> <b>FINAL PROVISIONS</b>	<b>CHAPTER X</b> <b>FINAL PROVISIONS</b>	
		<i>Article 70a</i>	
		<i>Processing of personal data and public access to documents</i>	
		Union institutions and bodies shall reconcile the right to the protection of personal data with the right of access to documents in accordance with Union law.	Moved to Article 9(3).
<i>Article 71</i>	<i>Article 71</i>	<i>Article 71</i>	
<i>Repeal of Regulation (EC) No 45/2001 and of Decision No 1247/2002/EC</i>	<i>Repeal of Regulation (EC) No 45/2001 and of Decision No 1247/2002/EC</i>	<i>Repeal of Regulation (EC) No 45/2001 and of Decision No 1247/2002/EC</i>	
Regulation (EC) No 45/2001 <sup>13</sup> and Decision No 1247/2002/EC <sup>14</sup> are repealed with effect from 25	Regulation (EC) No 45/2001 <sup>15</sup> and Decision No 1247/2002/EC <sup>16</sup> are repealed with effect from 25 May	1. Regulation (EC) No 45/2001 <sup>13</sup> and	Regulation (EC) No 45/2001 <sup>15</sup> and Decision No 1247/2002/EC <sup>16</sup> are repealed with effect from *.

<sup>13</sup> Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001.

<sup>14</sup> Decision No 1247/2002/EC of 1 July 2002 on the regulations and general conditions governing the performance of the European Data protection Supervisor's duties, OJ L 183, 12.07.2002, p. 1

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
May 2018. References to the repealed Regulation and Decision shall be construed as references to this Regulation.	2018. References to the repealed Regulation and Decision shall be construed as references to this Regulation.	Decision No 1247/2002/EC <sup>14</sup> are repealed with effect from 25 May 2018.	* (Date of entry into force of the Regulation)
		2. References to the repealed Regulation and Decision shall be construed as references to this Regulation.	References to the repealed Regulation and Decision shall be construed as references to this Regulation.
<i>Article 72</i>	<i>Article 72</i>	<i>Article 72</i>	
<i>Transitional measures</i>	<i>Transitional measures</i>	<i>Transitional measures</i>	
1. The Decision 2014/886/EU of the European Parliament and of the Council <sup>17</sup> and the current terms of office of the European Data Protection Supervisor and the Assistant Supervisor shall not be affected by this Regulation.	1. The Decision 2014/886/EU of the European Parliament and of the Council <sup>17</sup> and the current terms of office of the European Data Protection Supervisor and the Assistant Supervisor shall not be affected by this Regulation.	1. The Decision 2014/886/EU of the European Parliament and of the Council <sup>15</sup> and the current terms of office of the European Data Protection Supervisor and the Assistant Supervisor shall not be affected by this Regulation.	

<sup>15</sup> Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001.

<sup>16</sup> Decision No 1247/2002/EC of 1 July 2002 on the regulations and general conditions governing the performance of the European Data protection Supervisor's duties, OJ L 183, 12.07.2002, p. 1

<sup>17</sup> Decision 2014/886/EU of the European Parliament and of the Council of 4 December 2014 appointing the European Data Protection Supervisor and the Assistant Supervisor, OJ L 351, 09.12.2014, p.9.

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
2. The Assistant Supervisor shall be considered equivalent to the Registrar of the Court of Justice of the European Union as regards the determination of remuneration, allowances, retirement pension and any other benefit in lieu of remuneration.	2. The Assistant Supervisor shall be considered equivalent to the Registrar of the Court of Justice of the European Union as regards the determination of remuneration, allowances, retirement pension and any other benefit in lieu of remuneration.	2. The Assistant Supervisor shall be considered equivalent to the Registrar of the Court of Justice of the European Union as regards the determination of remuneration, allowances, retirement pension and any other benefit in lieu of remuneration.	
3. Article 54(4), (5) and (7), and Articles 56 and 57 of this Regulation shall apply to the current Assistant Supervisor until the end of his term of office on 5 December 2019.	3. Article 54(4), (5) and (7), and Articles 56 and 57 of this Regulation shall apply to the current Assistant Supervisor until the end of his term of office on 5 December 2019.	3. Article 54(4), (5) and (7), and Articles 56 and 57 of this Regulation shall apply to the current Assistant Supervisor until the end of his term of office on 5 December 2019.	
4. The Assistant Supervisor shall assist the European Data Protection Supervisor in all the latter's duties and act as a replacement when the European Data Protection Supervisor is absent or prevented from attending to those duties until the end of the Assistant Supervisor's term of office on 5 December 2019.	4. The Assistant Supervisor shall assist the European Data Protection Supervisor in all the latter's duties and act as a replacement when the European Data Protection Supervisor is absent or prevented from attending to those duties until the end of the Assistant Supervisor's term of office on 5 December 2019.	4. The Assistant Supervisor shall assist the European Data Protection Supervisor in all the latter's duties and act as a replacement when the European Data Protection Supervisor is absent or prevented from attending to those duties until the end of the Assistant Supervisor's term of office on 5 December 2019.	

COM (2017) 8	EP Position / First Reading	Council General Approach	Final compromise
<i>Article 73</i>	<i>Article 73</i>	<i>Article 73</i>	
<b><i>Entry into force and application</i></b>	<b><i>Entry into force and application</i></b>	<b><i>Entry into force and application</i></b>	
1. This Regulation shall enter into force on the twentieth day following that of its publication in the <i>Official Journal of the European Union</i> .	1. This Regulation shall enter into force on the twentieth day following that of its publication in the <i>Official Journal of the European Union</i> .	1. This Regulation shall enter into force on the twentieth day following that of its publication in the <i>Official Journal of the European Union</i> .	
2. It shall apply from 25 May 2018.	2. It shall apply from 25 May 2018.	2. It shall apply from 25 May 2018.	2.By way of derogation from paragraph 1, this Regulation shall apply to processing of personal data by Eurojust from the date of entry into application of Regulation (EU) 2018/ XXX [new Eurojust Regulation].