Council of the European Union

Brussels, 14 October 2015
(OR. en)

12493/15

Interinstitutional File:
2012/0010 (COD)

LIMITE

DATAPROTECT 152
JAI 698
DAPIX 160
FREMP 197
COMIX 449
CODEC 1264

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	12555/15
Subject:	Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data - Preparation of trilogues with the European Parliament

1. Delegations will find in the Annex the four-column table in order to prepare for the trilogues with the European Parliament on the above-mentioned Directive.

2. The Commission proposal (5833/12) is set out in the first column. The second column contains the position of the European Parliament (7428/14) with changes highlighted in ***bold italics*** and strikethrough for deleted text. The third column sets out the position of the Council as in the general approach of 9 October 2015 (12555/15) with changes highlighted in underline and (…) for deleted text as compared to the Commission proposal.

ANNEX

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
Proposal for a	Proposal for a	Proposal for a	
DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL	DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL	DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL	
on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data	on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data	on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties**,** or the safeguarding against and the prevention of threats to public security, and the free movement of such data	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN 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,	
After consulting the European Data Protection Supervisor[1], [1] OJ C… , p. .	***Having regard to the opinion of*** the European Data Protection Supervisor[1], [1] OJ C 192, 30.6.2012, p.7.	After consulting the European Data Protection Supervisor[1], [1] OJ C… , p. .	
Acting in accordance with the ordinary legislative procedure,	Acting in accordance with the ordinary legislative procedure[2], ***2*** *Position of the European Parliament of 12 March 2014.*	Acting in accordance with the ordinary legislative procedure,	
Whereas:	Whereas:	Whereas:	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
	Amendment 1		
(1) The protection of natural persons in relation to the processing of personal data is fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty of the Functioning of the European Union lay down that everyone has the right to the protection of personal data concerning him or her.	(1) 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 ***('Charter')*** and Article 16(1) of the Treaty of the Functioning of the European Union lay down that everyone has the right to the protection of personal data concerning them. ***Article 8(2) of the Charter lays down that such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.***	(1) 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 and Article 16(1) of the Treaty of the Functioning of the European Union lay down that everyone has the right to the protection of personal data concerning him or her.	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
(2) The processing of personal data is designed to serve man; the principles and rules on the protection of individuals with regard to the processing of their personal data should, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably their right to the protection of personal data. It should contribute to the accomplishment of an area of freedom, security and justice.	(2) The processing of personal data is designed to serve man; the principles and rules on the protection of individuals with regard to the processing of their personal data should, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably their right to the protection of personal data. It should contribute to the accomplishment of an area of freedom, security and justice.	(2) The (…) principles and rules on the protection of individuals with regard to the processing of their personal data should, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably their right to the protection of personal data. It should contribute to the accomplishment of an area of freedom, security and justice.	
(3) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of data collection and sharing has increased spectacularly. Technology allows competent authorities to make use of personal data on an unprecedented scale in order to pursue their activities.	(3) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of data collection and sharing has increased spectacularly. Technology allows competent authorities to make use of personal data on an unprecedented scale in order to pursue their activities.	(3) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of data collection and sharing has increased spectacularly. Technology allows (…) to make use of personal data on an unprecedented scale in order to pursue (…) activities <u>such as the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.</u>	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
	Amendment 2		
(4) This requires facilitating the free flow of data between competent authorities within the Union and the transfer to third countries and international organisations, while ensuring a high level of protection of personal data. These developments require building a strong and more coherent data protection framework in the Union, backed by strong enforcement.	(4) This requires facilitating the free flow of data***, when necessary and proportionate,*** between competent authorities within the Union and the transfer to third countries and international organisations, while ensuring a high level of protection of personal data. These developments require building a strong and more coherent data protection framework in the Union, backed by strong enforcement.	(4) This requires facilitating the free flow of data between competent authorities <u>for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal</u> penalties <u>or the safeguarding against and the prevention of threats to public security</u> within the Union and the transfer to third countries and international organisations, while ensuring a high level of protection of personal data. These developments require building a strong and more coherent data protection framework in the Union, backed by strong enforcement.	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
(5) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[2] applies to all personal data processing activities in Member States in both the public and the private sectors. However, it does not apply to the processing of personal data 'in the course of an activity which falls outside the scope of Community law', such as activities in the areas of judicial co-operation in criminal matters and police co-operation. [2] OJ L 281, 23.11.1995, p. 31.	(5) Directive 95/46/EC of the European Parliament and of the Council[1] applies to all personal data processing activities in Member States in both the public and the private sectors. However, it does not apply to the processing of personal data in the course of an activity which falls outside the scope of Community law, such as activities in the areas of judicial co-operation in criminal matters and police co-operation. [1] ***Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).***	(5) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[2] applies to all personal data processing activities in Member States in both the public and the private sectors. However, it does not apply to the processing of personal data 'in the course of an activity which falls outside the scope of Community law', such as activities in the areas of judicial co-operation in criminal matters and police co-operation. [2] OJ L 281, 23.11.1995, p. 31.	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
(6) Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters[1] applies in the areas of judicial co-operation in criminal matters and police co-operation. The scope of application of this Framework Decision is limited to the processing of personal data transmitted or made available between Member States. [1] OJ L 350, 30.12.2008, p. 60.	(6) Council Framework Decision 2008/977/JHA**[1]** applies in the areas of judicial co-operation in criminal matters and police co-operation. The scope of application of this Framework Decision is limited to the processing of personal data transmitted or made available between Member States. **[1] *Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters (OJ L 350, 30.12.2008, p. 60).***	(6) Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters[3] applies in the areas of judicial co-operation in criminal matters and police co-operation. The scope of application of this Framework Decision is limited to the processing of personal data transmitted or made available between Member States. [3] OJ L 350, 30.12.2008, p. 60.	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
	Amendment 3		
(7) Ensuring a consistent and high level of protection of the personal data of individuals and facilitating the exchange of personal data between competent authorities of Members States is crucial in order to ensure effective judicial co-operation in criminal matters and police cooperation. To that aim, the level of protection of the rights and freedoms of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties must be equivalent in all Member States. Effective protection of personal data throughout the Union requires strengthening the rights of data subjects and the obligations of those who process personal data, but also equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data in the	(7) Ensuring a consistent and high level of protection of the personal data of individuals and facilitating the exchange of personal data between competent authorities of Members States is crucial in order to ensure effective judicial co-operation in criminal matters and police cooperation. To that aim, the level of protection of the rights and freedoms of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties must be equivalent in all Member States. ***Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union.*** Effective protection of personal data throughout the Union	(7) Ensuring a consistent and high level of protection of the personal data of individuals and facilitating the exchange of personal data between competent authorities of Members States is crucial in order to ensure effective judicial co-operation in criminal matters and police cooperation. To that aim, the level of protection of the rights and freedoms of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties or the safeguarding against and the prevention of threats to public security should be equivalent in all Member States. Effective protection of personal data throughout the Union requires strengthening the rights of data subjects and the obligations of those who process personal data, but also equivalent	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
Member States.	requires strengthening the rights of data subjects and the obligations of those who process personal data, but also equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data in the Member States.	powers for monitoring and ensuring compliance with the rules for the protection of personal data in the Member States.	
	Amendment 4		
(8) Article 16(2) of the Treaty on the Functioning of the European Union provides that the European Parliament and the Council should lay down the rules relating to the protection of individuals with regard to the processing of personal data and the rules relating to the free movement of personal data.	(8) Article 16(2) of the Treaty on the Functioning of the European Union provides that the European Parliament and the Council should lay down the rules relating to the protection of individuals with regard to the processing of personal data and the rules relating to the free movement of ***their*** personal data.	(8) Article 16(2) of the Treaty on the Functioning of the European Union mandates the European Parliament and the Council to lay down the rules relating to the protection of individuals with regard to the processing of personal data and the rules relating to the free movement of personal data.	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
(9) On that basis, Regulation EU …../2012 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) lays down general rules to protect of individuals in relation to the processing of personal data and to ensure the free movement of personal data within the Union.	(9) On that basis, Regulation (EU) No …/2014 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) lays down general rules to protect of individuals in relation to the processing of personal data and to ensure the free movement of personal data within the Union.	(9) On that basis, Regulation EU …../XXX of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) lays down general rules to protect (…) individuals in relation to the processing of personal data and to ensure the free movement of personal data within the Union.	
(10) In Declaration 21 on the protection of personal data in the fields of judicial co-operation in criminal matters and police co-operation, 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 such data in the fields of judicial co-operation in	(10) In Declaration 21 on the protection of personal data in the fields of judicial co-operation in criminal matters and police co-operation, 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 such data in the fields of judicial co-operation in	(10) In Declaration 21 on the protection of personal data in the fields of judicial co-operation in criminal matters and police co-operation, 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 such data in the fields of judicial co-operation in	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
criminal matters and police co-operation based on Article 16 of the Treaty on the Functioning of the European Union may prove necessary because of the specific nature of these fields.	criminal matters and police co-operation based on Article 16 of the Treaty on the Functioning of the European Union may prove necessary because of the specific nature of these fields.	criminal matters and police co-operation based on Article 16 of the Treaty on the Functioning of the European Union may prove necessary because of the specific nature of these fields.	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
	Amendment 5		
(11) Therefore a distinct Directive should meet the specific nature of these fields and lay down the rules relating to the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.	(11) Therefore a ~~distinct~~ ***specific*** Directive should meet the specific nature of these fields and lay down the rules relating to the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.	(11) Therefore a distinct Directive should meet the specific nature of these fields and lay down the rules relating to the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. Such competent authorities may include not only public authorities such as the judicial authorities, the police or other law enforcement authorities but also any body/entity entrusted by national law to perform public duties or exercise public powers for the purposes of prevention, investigation, detection or prosecution of criminal offence or the execution of criminal penalties. However where such body/entity processes personal data for other purposes than for the performance of public duties and/or the exercise of public powers for	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
		the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, Regulation EU/XXX applies. Therefore Regulation EU/XXX applies in cases where a body/entity**,** collects personal data for other purposes and further processes those personal data for compliance with a legal obligation to which it is subject e.g. financial institutions retain for the purpose of investigation, detection and prosecutions certain data which are processed by them, and provide those data only to the competent national authorities in specific cases and in accordance with national law. A body/entity which processes personal data on behalf of such authorities within the scope of this Directive should be bound, by a contract or other legal act and the provisions applicable to processors pursuant to this Directive, while the application of Regulation EU/XXX remains unaffected for processing activities of the processor outside the scope of this Directive.	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
		(11a) The activities carried out by the police or other law enforcement authorities are mainly focused on the prevention, investigation, detection or prosecution of criminal offences including police activities without prior knowledge if an incident is a criminal offence or not. These can also include the exercise of authority by taking coercive measures such as police activities at demonstrations, major sporting events and riots. Those activities performed by the above-mentioned authorities also include maintaining law and order as a task conferred on the police or other law enforcement authorities where necessary to safeguard against and prevent threats to public security, aimed at preventing human behaviour which may lead to threats to fundamental interests of the society protected by the law and which may lead to a criminal offence.	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
		Member States may entrust competent authorities with other tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the safeguarding against and prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of Regulation EU/XXX.	
		(11aa) The concept of a criminal offence within the meaning of this Directive should be an autonomous concept of Union law as interpreted by the Court of Justice of the European Union.	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
		(11b) Since this Directive should not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law, activities concerning national security, activities of agencies or units dealing with national security issues and processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union should not be considered as activities falling under the scope of this Directive.	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
(12) In order to ensure the same level of protection for individuals through legally enforceable rights throughout the Union and to prevent divergences hampering the exchange of personal data between competent authorities, the Directive should provide harmonised rules for the protection and the free movement of personal data in the areas of judicial co-operation in criminal matters and police co-operation.	(12) In order to ensure the same level of protection for individuals through legally enforceable rights throughout the Union and to prevent divergences hampering the exchange of personal data between competent authorities, this Directive should provide harmonised rules for the protection and the free movement of personal data in the areas of judicial co-operation in criminal matters and police co-operation.	(12) In order to ensure the same level of protection for individuals through legally enforceable rights throughout the Union and to prevent divergences hampering the exchange of personal data between competent authorities, the Directive should provide harmonised rules for the protection and the free movement of personal data (…) processed for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties or the safeguarding against and the prevention of threats to public security. The approximation of Member States' laws should not result in any lessening of the data protection they afford but should, on the contrary, seek to ensure a high level of protection within the Union. Member States should not be precluded from providing higher safeguards than those established in	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
		this Directive for the protection of the rights and freedoms of the data subject with regard to the processing of personal data by competent authorities.	
(13) This Directive allows the principle of public access to official documents to be taken into account when applying the provisions set out in this Directive.	(13) This Directive allows the principle of public access to official documents to be taken into account when applying the provisions set out in this Directive.	(13) This Directive is without prejudice to the principle of public access to official documents (…). Under Regulation EU/XXX personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union law or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data.	
(14) The protection afforded by this Directive should concern natural persons, whatever their nationality or place of residence, in relation to the processing of personal data.	(14) The protection afforded by this Directive should concern natural persons, whatever their nationality or place of residence, in relation to the processing of personal data.	(14) The protection afforded by this Directive should concern natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data.	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
	Amendment 6		
(15) The protection of individuals should be technological neutral and not depend on the techniques used; otherwise this would create a serious risk of circumvention. The protection of individuals should apply to processing of personal data by automated means, as well as to manual processing if the 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 Directive. This Directive should not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law, in particular concerning national security, or to data processed by the Union institutions, bodies, offices and agencies, such as Europol or Eurojust.	(15) The protection of individuals should be technological neutral and not depend on the techniques used; otherwise this would create a serious risk of circumvention. The protection of individuals should apply to processing of personal data by automated means, as well as to manual processing if the 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 Directive. This Directive should not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law~~, in particular concerning national security, or to data processed by the Union institutions, bodies, offices and agencies, such as Europol or~~	(15) The protection of individuals should be technologically neutral and not depend on the technologies used; otherwise this would create a serious risk of circumvention. The protection of individuals should apply to processing of personal data by automated means, as well as to manual processing if the 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 Directive.	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
	~~Eurojust~~. ***Regulation (EC) No 45/2001 of the European Parliament and of the Council[1] and specific legal instruments applicable to Union agencies, bodies or offices should be brought in line with this Directive and applied in accordance with this Directive.*** ***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, p. 1).***		

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
		(15a) Regulation (EC) No 45/2001[4] applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Regulation (EC) No 45/2001 and other Union legal instruments applicable to such processing of personal data should be adapted to the principles and rules of Regulation EU/XXX. [4]OJ L 8, 12.1.2001, p. 1.	
		(15b) This Directive does not preclude Member States from specifying processing operations and processing procedures in national rules on criminal procedures in relation to the processing of personal data by courts and other judicial authorities, in particular as regards personal data contained in a judicial decision or in records in relation to criminal proceedings.	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
	Amendment 7		
(16) The principles of protection should apply to any information concerning an identified or identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the individual. The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.	(16) The principles of protection should apply to any information concerning an identified or identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify ***or single out*** the individual. The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable. ***This Directive should not apply to anonymous data, meaning any data that cannot be related, directly or indirectly, alone or in combination with associated data, to a natural person. Given the importance of the developments under way in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate***	(16) The principles of <u>data</u> protection should apply to any information concerning an identified or identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the individual <u>directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the individual, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development.</u> The principles of data protection should <u>therefore</u> not apply to <u>anonymous information, that is information which does not relate to an identified or identifiable</u>	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
	location data relating to natural persons, which may be used for different purposes including surveillance or creating profiles, this Directive should be applicable to processing involving such personal data.	natural person or to data rendered anonymous in such a way that the data subject is no longer identifiable.	
	Amendment 8		
	(16a) Any processing of personal data must be lawful, fair and transparent in relation to the individuals concerned. In particular, the specific purposes for which the 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 the minimum necessary for the	(16a) Genetic data should be defined as personal data relating to the genetic characteristics of an individual which have been inherited or acquired which give unique information about the physiology or health of that individual, resulting in particular by chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis or analysis of any other element enabling equivalent information to be obtained.	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
	purposes for which the personal data are processed. This requires in particular limiting the data collected and the period for which the data are stored to a strict minimum. Personal data should only be processed if the purpose of the processing could not be fulfilled by other means. Every reasonable step should be taken to ensure that personal data which are inaccurate should be rectified or deleted. In order to ensure that the data are kept no longer than necessary, time limits should be established by the controller for erasure or periodic review.		

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
(17) Personal data relating to health should include in particular all data pertaining to the health status of a data subject, information about the registration of the individual for the provision of health services; information about payments or eligibility for healthcare with respect to the individual; a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; any information about the individual collected in the course of the provision of health services to the individual; information derived from the testing or examination of a body part or bodily substance, including biological samples; identification of a person as provider of healthcare to the individual; or any information on, for example; a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of	(17) Personal data relating to health should include in particular all data pertaining to the health status of a data subject, information about the registration of the individual for the provision of health services; information about payments or eligibility for healthcare with respect to the individual; a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; any information about the individual collected in the course of the provision of health services to the individual; information derived from the testing or examination of a body part or bodily substance, including biological samples; identification of a person as provider of healthcare to the individual; or any information on, for example; a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of	(17) Personal data <u>concerning</u> health should include (…) data pertaining to the health status of a data subject <u>which reveal information relating to the past, current or future physical or mental health of the data subject; including</u> information about the registration of the individual for the provision of health services; (…) a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; (…) information derived from the testing or examination of a body part or bodily substance, including <u>genetic data and</u> biological samples<u>;</u> (…) or any <u>i</u>nformation on, for example, a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, <u>such as for example</u> from a physician or other health professional, a hospital, a medical	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
the data subject independent of its source, e.g. from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.	the data subject independent of its source, e.g. from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.	device, or an in vitro diagnostic test.	
	Amendment 9		
(18) Any processing of personal data must be fair and lawful in relation to the individuals concerned. In particular, the specific purposes for which the data are processed should be explicit.	***deleted***	(18) Any processing of personal data must be lawful *and fair* in relation to the individuals concerned, and only processed for specific purposes laid down by law. The principle of fair processing does not in itself prevent the law enforcement authorities from carrying out activities such as covert investigations or video surveillance. Such activities can be done for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties or the safeguarding against and the prevention of threats to public security as long as they are laid down by law and	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
		constitute a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the individual concerned. The data protection principle of fair processing is a distinct notion from the right to a fair trial as defined by Article 6 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and Article 47 of the Charter of Fundamental Rights. Individuals should be made aware of risks, rules, safeguards and rights in relation to the processing of his/her personal data and how to exercise his or her rights in relation to the processing. In particular, the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the collection of the data. The data should be adequate and relevant for the purposes for which the data are processed; this requires, in	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
		particular, ensuring that the data collected are not excessive and not kept longer than is necessary for the purpose for which they are processed. Personal data should only be processed if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Member States should lay down appropriate safeguards for personal data stored for longer periods for archiving in the public interest, scientific, statistical or historical use.	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
	Amendment 10		
(19) For the prevention, investigation and prosecution of criminal offences, it is necessary for competent authorities to retain and process personal data, collected in the context of the prevention, investigation, detection or prosecution of specific criminal offences beyond that context to develop an understanding of criminal phenomena and trends, to gather intelligence about organised criminal networks, and to make links between different offences detected.	***deleted***	(19) For the prevention, investigation and prosecution of criminal offences it is necessary for competent authorities to (…) process personal data, collected in the context of the prevention, investigation, detection or prosecution of specific criminal offences beyond that context to develop an understanding of criminal phenomena and trends, to gather intelligence about organised criminal networks, and to make links between different offences detected.	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
		(19a) In order to maintain security of the processing and to prevent processing in breach of this Directive, personal data should be processed in a manner that ensures an appropriate level of security and confidentiality, including preventing unauthorised access to or use of personal data and the equipment used for the processing, taking into account available state of the art and technology and the costs of implementation in relation to the risks and the nature of the personal data to be protected.	
	Amendment 11		
(20) Personal data should not be processed for purposes incompatible with the purpose for which it was collected. Personal data should be adequate, relevant and not excessive for the purposes for which the personal data are processed. Every reasonable step should be taken to ensure that personal data which are inaccurate should be rectified or erased.	***deleted***	(20) (…)	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
	Amendment 12		
	(20a) The simple fact that two purposes both relate to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties does not necessarily mean that they are compatible. However, there are cases in which further processing for incompatible purposes should be possible if necessary to comply with a legal obligation to which the controller is subject, in order to protect the vital interests of the data subject or another person, or for the prevention of an immediate and serious threat to public security. Member States should therefore be able to adopt national laws providing for such derogations to the extent strictly necessary. Such national laws should contain adequate safeguards.	(20a) Personal data should be collected for specified, explicit and legitimate purposes within the scope of this Directive and not be processed for purposes incompatible with the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties or the safeguarding against and the prevention of threats to public security. If personal data is processed by the same or another controller for a purpose within the scope of this Directive other than the one for which it has been collected, such processing is compatible under the conditions that this processing is authorised in accordance with the applicable legal provisions and is necessary and proportionate to that other purpose.	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
(21) The principle of accuracy of data should be applied taking account of the nature and purpose of the processing concerned. In particular in judicial proceedings, statements containing personal data are based on the subjective perception of individuals and are in some cases not always verifiable. Consequently, the requirement of accuracy should not appertain to the accuracy of a statement but merely to the fact that a specific statement has been made.	(21) The principle of accuracy of data should be applied taking account of the nature and purpose of the processing concerned. In particular in judicial proceedings, statements containing personal data are based on the subjective perception of individuals and are in some cases not always verifiable. Consequently, the requirement of accuracy should not appertain to the accuracy of a statement but merely to the fact that a specific statement has been made.	(21) The principle of accuracy of data should be applied taking account of the nature and purpose of the processing concerned. (…) Since *personal data relating to different categories of data subjects are processed, the competent (...) authorities should, as far as possible, make a distinction between personal data of different categories of data subjects such as persons convicted of a criminal offence, suspects, (...) victims and third parties*. In particular in judicial proceedings, statements containing personal data are based on the subjective perception of individuals and are in some cases not always verifiable. Consequently, the requirement of accuracy should not appertain to the accuracy of a statement but merely to the fact that a specific statement has been made.	Text in italics moved from recital (23)

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
	Amendment 13		
(22) In the interpretation and application of the general principles relating to personal data processing by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, account should be taken of the specificities of the sector, including the specific objectives pursued.	***deleted***	(22) In the interpretation and application of the provisions of this Directive, by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties or the safeguarding against and the prevention of threats of public security, account should be taken of the specificities of the sector, including the specific objectives pursued.	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
	Amendment 14		
(23) It is inherent to the processing of personal data in the areas of judicial co-operation in criminal matters and police co-operation that personal data relating to different categories of data subjects are processed. Therefore a clear distinction should as far as possible be made between personal data of different categories of data subjects such as suspects, persons convicted of a criminal offence, victims and third parties, such as witnesses, persons possessing relevant information or contacts and associates of suspects and convicted criminals.	(23) It is inherent to the processing of personal data in the areas of judicial co-operation in criminal matters and police co-operation that personal data relating to different categories of data subjects are processed. Therefore a clear distinction should as far as possible be made between personal data of different categories of data subjects such as suspects, persons convicted of a criminal offence, victims and third parties, such as witnesses, persons possessing relevant information or contacts and associates of suspects and convicted criminals. ***Specific rules on the consequences of this categorisation should be provided by the Member States, taking into account the different purposes for which data are collected and providing specific safeguards for persons who are not suspected of having committed, or have not been convicted of, a criminal offence.***	(23) deleted	Moved to recital (21)

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
(24) As far as possible personal data should be distinguished according to the degree of their accuracy and reliability. Facts should be distinguished from personal assessments, in order to ensure both the protection of individuals and the quality and reliability of the information processed by the competent authorities.	(24) As far as possible personal data should be distinguished according to the degree of their accuracy and reliability. Facts should be distinguished from personal assessments, in order to ensure both the protection of individuals and the quality and reliability of the information processed by the competent authorities.	(24) (…) The competent authorities should ensure that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. In order to ensure both the protection of individuals and the accuracy, completeness or up-to-datedness and reliability of the personal data transmitted or made available (…) the competent authorities should, as far as possible, add necessary information in all transmissions of personal data.	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
		(24a) Wherever this Directive refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant the constitutional order of the Member State concerned, however, such legal basis or legislative measure should be clear and precise and its application foreseeable for those subject to it as required by the case law of the Court of Justice of the European Union and the European Court on Human Rights.	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
		(24b) 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 or the safeguarding against and the prevention of threats to public security should cover any operation or set of operations which is performed upon personal data or sets of personal data for those purposes, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, alignment or combination, restriction, erasure or destruction. In particular, the rules of this Directive should apply to the transmission of personal data for the purposes of this Directive to a recipient not subject to this Directive. Such recipient should mean a natural or legal person, public authority, agency or any other body, to which the data are lawfully disclosed by the competent authority.	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
		Where data were initially collected by a competent authority for one of the purposes of this Directive, Regulation EU/XXX should apply to the processing of this data for purposes other than the purposes of this Directive where such processing is authorized by Union or Member State law. In particular, the rules of the Regulation EU/XXX should apply to the transmission of personal data for purposes outside the scope of this Directive. For the processing of personal data by a recipient who is not or is not acting as a competent authority in the meaning of this Directive and to whom personal data are lawfully disclosed by a competent authority, Regulation EU/XXX should apply. While implementing this Directive, Member States may also further specify the application of the rules of the Regulation EU/XXX, subject to the conditions set out in the Regulation EU/XXX.	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
	Amendment 15		
(25) In order to be lawful, the processing of personal data should be necessary for compliance with a legal obligation to which the controller is subject, for the performance of a task carried out in the public interest by a competent authority based on law or in order to protect the vital interests of the data subject or of another person, or for the prevention of an immediate and serious threat to public security.	(25) In order to be lawful, the processing of personal data should be ***only allowed when*** necessary for compliance with a legal obligation to which the controller is subject, for the performance of a task carried out in the public interest by a competent authority based on ***Union or Member State*** law ~~or in order to protect the vital interests of the data subject or of another person, or for the prevention of an immediate and serious threat to public security~~ ***which should contain explicit and detailed provisions at least as to the objectives, the personal data, the specific purposes and means, designate or allow to designate the controller, the procedures to be followed, the use and limitations of the scope of any discretion conferred to the competent authorities in relation to the processing activities***.	(25) In order to be lawful, the processing of personal data under this Directive should be necessary for (…) the performance of a task carried out in the public interest by a competent authority based on Union law or Member State law for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties or the safeguarding against and the prevention of threats to public security**,** including processing necessary (…) in order to protect the vital interests of the data subject or of another person (…). The performance of the task of preventing, investigating, detecting or prosecuting criminal offences institutionally conferred by law to the competent authorities allows them to require/order individuals to abide to the requests made. In this case**,** the data subject's consent (as defined in Regulation EU/XXX) should not provide a legal ground	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
		for processing personal data by competent authorities. Where the data subject is required to comply with a legal obligation, the data subject has no genuine and free choice, so that the data subject's reaction could not be considered as a freely-given indication of his or her wishes. This should not preclude Member States to provide by law that the data subject may agree to the processing of his/her personal data for the purposes of this Directive, such as DNA tests in criminal investigations or monitoring of the data subject's location with electronic tags for the execution of criminal penalties.	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
	Amendment 16		
	(25a) Personal data should not be processed for purposes incompatible with the purpose for which they were collected. Further processing by competent authorities for a purpose falling within the scope of this Directive which is not compatible with the initial purpose should only be authorised in specific cases where such processing is necessary for compliance with a legal obligation, based on Union or Member State law, to which the controller is subject, or in order to protect the vital interests of the data subject or of another person or for the prevention of an immediate and serious threat to public security. The fact that data are processed for a law enforcement purpose does not necessarily imply that this	(25a) Member States should provide that where Union law or the national law applicable to the transmitting competent authority provides for specific conditions applicable in specific circumstances to the processing of personal data, such as for example the use of handling codes the transmitting authority should inform the recipient to whom data are transmitted about such conditions and the requirement to respect them. Such conditions may for example include that the recipient to whom the data are transmitted does not transmit further the data or use it for other purposes or does not inform the data subject in case of a limitation to the right of information without the prior approval of the transmitting competent authority. These obligations apply also to transfers the transmitting competent	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
	purpose is compatible with the initial purpose. The concept of compatible use is to be interpreted restrictively.	to recipients in third countries or international organisations. Member States should provide that authority does not apply such conditions to recipients in other Member States or to agencies, offices and bodies established pursuant to Chapters IV and V of Title V of the Treaty on the Functioning of the European Union other than those applicable to similar data transmissions within the Member State of the transmitting competent authority.	
	Amendment 17		
	(25b) Personal data processed in breach of the national provisions adopted pursuant to this Directive should not be further processed.		

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
	Amendment 18		
(26) Personal data which are, by their nature, particularly sensitive in relation to fundamental rights or privacy, including genetic data, deserve specific protection. Such data should not be processed, unless processing is specifically authorised by a law which provides for suitable measures to safeguard the data subject's legitimate interests; or processing is necessary to protect the vital interests of the data subject or of another person; or the processing relates to data which are manifestly made public by the data subject.	(26) Personal data which are, by their nature, particularly sensitive ***and vulnerable*** in relation to fundamental rights or privacy~~,~~ ~~including genetic data,~~ deserve specific protection. Such data should not be processed, unless processing is specifically ~~authorised by a~~ ***necessary for the performance of a task carried out in the public interest, on the basis of Union or Member State*** law which provides for suitable measures to safeguard the data subject's ***fundamental rights and*** legitimate interests; or processing is necessary to protect the vital interests of the data subject or of another person; or the processing relates to data which are manifestly made public by the data subject. ***Sensitive personal data should be processed only if they supplement other personal data already processed for law enforcement purposes. Any derogation to the prohibition of***	(26) Personal data which are, by their nature, particularly sensitive in relation to fundamental rights (…) and freedoms, (…), deserve specific protection as the context of their processing may create important risks for the fundamental rights and freedoms. These data should also include personal data revealing racial or ethnic origin, whereby the use of the term 'racial origin' in this Directive does not imply an acceptance by the European Union of theories which attempt to determine the existence of separate human races. Such data should not be processed, unless processing is subject to appropriate safeguards for the rights and freedoms of the data subject laid down by law and is allowed in cases authorised by law; or if not already authorised by such a law the processing is necessary to protect the vital interests of the data subject or of another person; or	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
	processing of sensitive data should be interpreted restrictively and not lead to frequent, massive or structural processing of sensitive personal data.	the processing relates to data which is manifestly made public by the data subject. Appropriate safeguards for the rights and freedoms of the data subject may for example include the possibility to collect those data only in connection with other data on the individual concerned, to adequately secure the data collected, stricter rules on the access of staff of the competent authority to the data, or the prohibition of transmission of those data. Processing of such data should also be allowed by law when the data subject has explicitly agreed in cases where the processing of data is particularly intrusive for the persons. However, the agreement of the data subject should not provide in itself a legal ground for processing such sensitive personal data by competent authorities.	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
	Amendment 19		
	(26a) The processing of genetic data should only be allowed if there is a genetic link which appears in the course of a criminal investigation or a judicial procedure. Genetic data should only be stored as long as strictly necessary for the purpose of such investigations and procedures, while Member States can provide for longer storage under the conditions set out in this Directive.		

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
	Amendment 20		
(27) Every natural person should have the right not to be subject to a measure which is based solely on automated processing if it produces an adverse legal effect for that person, unless authorised by law and subject to suitable measures to safeguard the data subject's legitimate interests.	(27) Every natural person should have the right not to be subject to a measure which is based solely on ***partially or fully profiling by means of*** automated processing ~~if it~~. ***Such processing which*** produces ~~an adverse~~ ***a*** legal effect for that person, ***or significantly affects him or her should be prohibited,*** unless authorised by law and subject to suitable measures to safeguard the data subject's ***fundamental rights and*** legitimate interests***, including the right to be provided with meaningful information about the logic used in the profiling. Such processing should in no circumstances contain, generate, or discriminate based on special categories of data***.	(27) The data subject should have the right not to be subject to a decision evaluating personal aspects relating to him or her which is based solely on automated processing,(…) which produces adverse legal effects concerning him or her or significantly affects him or her. In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human intervention, in particular to express his or her point of view, to get an explanation of the decision reached after such assessment or the right to contest the decision.	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
	Amendment 21		
(28) In order to exercise their rights, any information to the data subject should be easily accessible and easy to understand, including the use of clear and plain language.	(28) In order to exercise his or her rights, any information to the data subject should be easily accessible and easy to understand, including the use of clear and plain language. ***This information should be adapted to the needs of the data subject in particular when information is addressed specifically to a child.***	(28) In order to exercise their rights, any information to the data subject should be easily accessible, <u>including on the website of the controller</u> and easy to understand, <u>requiring</u> the use of clear and plain language.	
	Amendment 22		
(29) Modalities should be provided for facilitating the data subject's exercise of their rights under this Directive, including mechanisms to request, free of charge, in particular access to data, rectification and erasure. The controller should be obliged to respond to requests of the data subject without undue delay.	(29) Modalities should be provided for facilitating the data subject's exercise of his or her rights under this Directive, including mechanisms to request, free of charge, in particular access to data, rectification and erasure. The controller should be obliged to respond to requests of the data subject without ~~undue~~ delay ***and within one month of receipt of the request. Where personal data are***	(29) Modalities should be provided for facilitating the data subject's exercise of <u>his or her</u> rights under <u>the provisions adopted pursuant to</u> this Directive, including mechanisms to request, free of charge (…) access to data, <u>as well as</u> rectification, erasure <u>and restriction.</u> The controller should be obliged to respond to requests of the data subject without undue delay. <u>However, if requests are</u>	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
	processed by automated means the controller should provide means for requests to be made electronically.	s manifestly unfounded or excessive such as when the data subject unreasonably and repetitiously requests information or where the data ubject abuses his or her right to receive information, for example, by providing false or misleading information when making the request, the controller could refuse to act on the request.	
	Amendment 23		
(30) The principle of fair processing requires that the data subjects should be informed in particular of the existence of the processing operation and its purposes, how long the data will be stored, on the existence of the right of access, rectification or erasure and on the right to lodge a complaint. Where the data are collected from the data subject, the data subject should also be informed whether they are obliged	(30) The principle of fair ***and transparent*** processing requires that the data subjects should be informed in particular of the existence of the processing operation and its purposes, ***its legal basis,*** how long the data will be stored, on the existence of the right of access, rectification or erasure and on the right to lodge a complaint. ***Furthermore the data subject should be informed if profiling takes place and its***	(30) (…) At least the following information should be made available to the data subject: the identity of the controller, the existence of the processing operation, the purposes of the processing, (…) and (…) the right to lodge a complaint. (…) This could take place on the website of the competent authority.	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
to provide the data and of the consequences, in cases they do not provide such data.	***intended consequences.*** Where the data are collected from the data subject, the data subject should also be informed whether he or she is obliged to provide the data and of the consequences, in cases he or she does not provide such data.		

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
(31) The information in relation to the processing of personal data relating to the data subject should be given to them at the time of collection, or, where the data are not obtained from the data subject, at the time of the recording or within a reasonable period after the collection having regard to the specific circumstances in which the data are processed.	(31) 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, or, where the data are not obtained from the data subject, at the time of the recording or within a reasonable period after the collection having regard to the specific circumstances in which the data are processed.	(31) deleted	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
	Amendment 24		
(32) Any person should have the right of access to data which has been collected concerning them, and to exercise this right easily, in order to be aware of and verify the lawfulness of the processing. Every data subject should therefore have the right to know about and obtain communication in particular of the purposes for which the data are processed, for what period, which recipients receive the data, including in third countries Data subjects should be allowed to receive a copy of their personal data which are being processed.	(32) Any person should have the right of access to data which have been collected concerning them, and to exercise this right easily, in order to be aware of and verify the lawfulness of the processing. Every data subject should therefore have the right to know about, and obtain communication in particular of, the purposes for which the data are processed, ***the legal basis,*** for what period, which recipients receive the data, including in third countries***, the intelligible information about the logic involved in any automated processing and its significant and envisaged consequences if applicable, and the right to lodge a complaint with the supervisory authority and its contact details.*** Data subjects should be allowed to receive a copy of their personal data which are being processed.	(32) A natural person should have the right of access to data which has been collected concerning <u>him or her</u>, and to exercise this right easily <u>and at reasonable intervals</u> in order to be aware of and verify the lawfulness of the processing. Every data subject should therefore have the right to know about and obtain communication in particular of the purposes for which the data are processed, for what period, <u>and</u> which recipients receive the data, including in third countries. <u>For that right to be complied with, it is sufficient that the applicant be in possession of a full summary of those data in an intelligible form, that is to say a form which allows that applicant to become aware of those data and to check that they are accurate and processed in compliance with this Directive, so that he or she may, where relevant, exercise the rights conferred on him or her by this Directive.</u>	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
	Amendment 25		
(33) Member States should be allowed to adopt legislative measures delaying, restricting or omitting the information of data subjects or the access to their personal data to the extent that and as long as such partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the person concerned, to avoid obstructing official or legal inquiries, investigations or procedures, to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or for the execution of criminal penalties, to protect public security or national security, or, to protect the data subject or the rights and freedoms of others.	(33) Member States should be allowed to adopt legislative measures delaying ***or*** restricting or omitting the information of data subjects or the access to their personal data to the extent that and as long as such partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the ***fundamental rights and the*** legitimate interests of the person concerned, to avoid obstructing official or legal inquiries, investigations or procedures, to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or for the execution of criminal penalties, to protect public security or national security, or, to protect the data subject or the rights and freedoms of others. ***The controller should assess by way of concrete and individual examination of each case if partial or complete restriction of the right of access should apply.***	(33) Member States should be allowed to adopt legislative measures delaying, restricting or omitting the information of data subjects or the access to their personal data to the extent that and as long as such (…) a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the individual concerned, to avoid obstructing official or legal inquiries, investigations or procedures, to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or for the execution of criminal penalties, to safeguard public security or national security, or to safeguard (…) the rights and freedoms of others.	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
(34) Any refusal or restriction of access should be set out in writing to the data subject including the factual or legal reasons on which the decision is based.	(34) Any refusal or restriction of access should be set out in writing to the data subject including the factual or legal reasons on which the decision is based.	(34) Any refusal or restriction of access should in principle be set out in writing to the data subject and include the factual or legal reasons on which the decision is based.	
	Amendment 26		
	(34a) Any restriction of the data subject's rights must be in compliance with the Charter and with the European Convention on Human Rights, as clarified by the case law of the Court of Justice of the European Union and the European Court of Human Rights, and in particular respect the essence of the rights and freedoms.		

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
	Amendment 27		
(35) Where Member States have adopted legislative measures restricting wholly or partly the right to access, the data subject should have the right to request that the competent national supervisory authority checks the lawfulness of the processing. The data subject should be informed of this right. When access is exercised by the supervisory authority on behalf of the data subject, the data subject should be informed by the supervisory authority at least that all necessary verifications by the supervisory authority have taken place and of the result as regards to the lawfulness of the processing in question.	(35) Where Member States have adopted legislative measures restricting wholly or partly the right to access, the data subject should have the right to request that the competent national supervisory authority checks the lawfulness of the processing. The data subject should be informed of this right. When access is exercised by the supervisory authority on behalf of the data subject, the data subject should be informed by the supervisory authority at least that all necessary verifications by the supervisory authority have taken place and of the result as regards to the lawfulness of the processing in question. ***The supervisory authority should also inform the data subject of the right to seek a judicial remedy.***	(35) deleted	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
	Amendment 28		
(36) Any person should have the right to have inaccurate personal data concerning them rectified and the right of erasure where the processing of such data is not in compliance with the main principles laid down in this Directive. Where the personal data are processed in the course of a criminal investigation and proceedings, rectification, the rights of information, access, erasure and restriction of processing may be carried out in accordance with national rules on judicial proceedings.	(36) Any person should have the right to have inaccurate ***or unlawfully processed*** personal data concerning them rectified and the right of erasure where the processing of such data is not in compliance with the ~~main principles~~ ***provisions*** laid down in this Directive. ***Such rectification, completion or erasure should be communicated to recipients to whom the data have been disclosed and to the third parties from which the inaccurate data originated. The controllers should also abstain from further dissemination of such data.*** Where the personal data are processed in the course of a criminal investigation and proceedings, rectification, the rights of information, access, erasure and restriction of processing may be carried out in accordance with national rules on judicial proceedings.	(36) A natural person should have the right to have inaccurate personal data concerning him or her rectified, in particular when pertaining to facts, and the right of erasure where the processing of such data is not in compliance with the provisions laid down in this Directive.(…) However, the right to rectification should not affect, for example, the content of a witness testimony. A natural person may also have the right to have an item of personal data restricted where the accuracy is contested. In particular, personal data should be restricted instead of erased if in a specific case there are reasonable grounds to believe that erasure could affect the legitimate interests of the data subject. In this case, restricted data should be processed only for the purpose which prevented their erasure**.** Methods to restrict processing of personal data	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
		could include, inter alia, moving the selected data to another processing system**,** for example for archiving purposes, or making the selected data unavailable. In automated filing systems the restriction of processing of personal data should in principle be ensured by technical means; the fact that the processing of personal data is restricted should be indicated in the system in such a way that it is clear that the processing of the personal data is restricted.	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
		(36a) Where the controller denies a data subject his or her right of access, rectification, erasure or restriction of processing, the data subject should have the right to request that the national supervisory authority checks the lawfulness of the processing. The data subject should be informed of this right. When the supervisory authority intervenes on behalf of the data subject, the data subject should be informed by the supervisory authority at least that all necessary verifications or reviews by the supervisory authority have taken place.	
		(36aa) *Where the personal data are processed in the course of a criminal investigation and* court *proceedings* in criminal matters, the exercise of the *rights of information, access,* rectification, *erasure and restriction of processing may be carried out in accordance with national rules on judicial proceedings.*	Moved from the second part of recital (36)

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
	Amendment 29		
(37) Comprehensive 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 ensure the compliance of processing operations with the rules adopted pursuant to this Directive.	(37) Comprehensive 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 ensure ~~the~~ ***and be obliged to be able to demonstrate*** compliance of ***each*** processing ~~operations~~ ***operation*** with the rules adopted pursuant to this Directive.	(37) 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 measures and be able to demonstrate (…) the compliance of processing activities with the (…) provisions adopted pursuant to this Directive. These measures should take into account the nature, scope, context and purposes of the processing and the risk for the rights and freedoms of data subjects. Where proportionate in relation to the processing activities, the measures should include the implementation of appropriate data protection policies. These policies should specify the application of the data protection provisions adopted pursuant to this Directive.	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
		(37a) Risks for the rights and freedoms of data subjects, of varying likelihood and severity, may result from data processing which could lead to physical, material or moral 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 data protected by professional secrecy, unauthorized reversal of pseudonymisation, or any other significant economic or social disadvantage; or where data subjects might be deprived of their rights and freedoms or 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 or data concerning health or sex life or criminal convictions and offences or related security measures; where personal aspects are	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
		evaluated, in particular analysing and prediction of aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable individuals, in particular of children, are processed; where processing involves a large amount of personal data and affects a large number of data subjects.	
		(37b) The likelihood and severity of the risk should be determined in function of the nature, scope, context and purposes of the data processing. Risk should be evaluated on an objective assessment, by which it is established whether data processing operations involve a high risk. A high risk is a particular risk of prejudice to the rights and freedoms of data subjects.	

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
(38) The protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organisational measures be taken to ensure that the requirements of the Directive are met. In order to ensure compliance with the provisions adopted pursuant to this Directive, the controller should adopt policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default.	(38) The protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organisational measures be taken to ensure that the requirements of this Directive are met. In order to ensure compliance with the provisions adopted pursuant to this Directive, the controller should adopt policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default.	(38) The protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organisational measures be taken to ensure that the requirements of the Directive are met. In order to <u>be able to demonstrate</u> compliance with the provisions adopted pursuant to this Directive, the controller should adopt <u>internal</u> policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default. <u>Such measures could consist inter alia of the use of pseudonymisation as soon as possible. The use of pseudonymisation for the purposes of this Directive can serve as a tool that could facilitate, in particular, the free flow of relevant data within the Area of Freedom, Security and Justice.</u>	

	Amendment 30		
(39) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors requires a clear attribution of the responsibilities under this Directive, including where a controller determines the purposes, conditions and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.	(39) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors requires a clear attribution of the responsibilities under this Directive, including where a controller determines the purposes~~, conditions~~ and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller. ***The data subject should have the right to exercise his or her rights under this Directive in respect of and against each of the joint controllers.***	(39) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities under this Directive, 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.	
		(39a) The carrying out of processing by a processor should be governed by a legal act including a contract binding the processor to the controller and stipulating in particular that the processor should act only on instructions from the controller.	

(40) Processing activities should be documented by the controller or processor, in order to monitor compliance with this Directive. Each controller and processor should be obliged to co-operate with the supervisory authority and make this documentation available upon request, so that it might serve for monitoring processing operations.	(40) Processing activities should be documented by the controller or processor, in order to monitor compliance with this Directive. Each controller and processor should be obliged to co-operate with the supervisory authority and make this documentation available upon request, so that it might serve for monitoring processing operations.	(40) Categories of personal data processing activities including transfers by way of appropriate safeguards and in specific situations should be (…) recorded by the controller and the processor, in order to monitor compliance with this Directive. Each controller and processor should be obliged to co-operate with the supervisory authority and make these records, on request, available to it, so that it might serve for monitoring processing operations.	
	Amendment 31		
	(40a) Every processing operation of personal data should be recorded in order to enable the verification of the lawfulness of the data processing, self-monitoring and ensuring proper data integrity and security. This record should be made available upon request to the supervisory authority for the purpose of monitoring compliance with the rules laid down in this Directive.	(40a) Logs should be kept at least for operations in automated processing systems such as collection, alteration, consultation, disclosure, combination or erasure. The logs should be used for verification of the lawfulness of the data processing, self-monitoring and for ensuring data integrity and data security. This does not preclude the use of the logs in accordance with Member State law for operational matters in the course of criminal investigations and proceedings.	

	Amendment 32		
	(40b) A data protection impact assessment should be carried out by the controller or processor, where the processing operations are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, which should include in particular the envisaged measures, safeguards and mechanisms to ensure the protection of personal data and for demonstrating compliance with this Directive. Impact assessments should concern relevant systems and processes of personal data processing operations, but not individual cases.		

	Amendment 33		
(41) In order to ensure effective protection of the rights and freedoms of data subjects by way of preventive actions, the controller or processor should consult with the supervisory authority in certain cases prior to the processing.	(41) In order to ensure effective protection of the rights and freedoms of data subjects by way of preventive actions, the controller or processor should consult with the supervisory authority in certain cases prior to the processing. ***Moreover, where a data protection impact assessment indicates that processing operations are likely to present a high degree of specific risks to the rights and freedoms of data subjects, the supervisory authority should be in a position to prevent, prior to the start of operations, a risky processing which is not in compliance with this Directive, and to make proposals to remedy such situation. Such consultation may equally take place in the course of the preparation either of a measure of the national parliament or of a measure based on such legislative measure which defines the nature of the processing and lays down appropriate safeguards.***	(41) In order to ensure effective protection of the rights and freedoms of data subjects (…) the controller or processor should consult with the supervisory authority in certain cases prior to <u>intended</u> processing.	

	Amendment 34		
	(41a) In order to maintain security and to prevent processing in breach of this Directive, the controller or processor should evaluate the risks inherent to the processing and implement measures to mitigate those risks. Those measures should ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks and the nature of the personal data to be protected. When establishing technical standards and organisational measures to ensure security of processing, technological neutrality should be promoted.		

	Amendment 35		
(42) A personal data breach may, if not addressed in an adequate and timely manner, result in harm, including reputational damage to the individual concerned. Therefore, as soon as the controller becomes aware that such a breach has occurred, it should notify the breach to the competent national authority. The individuals whose personal data or privacy could be adversely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the personal data or privacy of an individual where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation in connection with the processing of personal data.	(42) A personal data breach may, if not addressed in an adequate and timely manner, result in ***a substantial economic loss and social*** harm, including ~~reputational damage~~ ***identity fraud,*** to the individual concerned. Therefore, as soon as the controller becomes aware that such a breach has occurred, it should notify the breach to the competent national authority. The individuals whose personal data or privacy could be adversely affected by the breach should be notified without ~~undue~~ delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the personal data or privacy of an individual where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation in connection	(42) A personal data breach may, if not addressed in an adequate and timely manner, result in physical, material or moral damage to individuals**,** such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, damage to the reputation, unauthorized reversal of pseudonymisation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage to the individual concerned. Therefore, as soon as the controller becomes aware that (…) a personal data breach has occurred which may result in physical, material or moral damage, the controller should notify the breach to the supervisory authority without undue delay. The individuals whose (…) rights and	

	with the processing of personal data. ***The notification should include information about measures taken by the provider to address the breach, as well as recommendations for the subscriber or individual concerned. Notifications to data subjects should be made as soon as feasible and in close cooperation with the supervisory authority and respecting guidance provided by it.***	freedoms (…) could be severely affected by the breach should be informed without undue delay in order to allow them to take the necessary precautions (…).	

(43) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of the breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of misuse. Moreover, such rules and procedures should take into account the legitimate interests of competent authorities in cases where early disclosure could unnecessarily hamper the investigation of the circumstances of a breach.	(43) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of the breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of misuse. Moreover, such rules and procedures should take into account the legitimate interests of competent authorities in cases where early disclosure could unnecessarily hamper the investigation of the circumstances of a breach.	(43) (…) The communication of a personal data breach to the data subject should not be required if the controller has implemented appropriate technological protection measures, and that those measures were applied to the data affected by the personal data breach. Such technological protection measures should include those that render the data unintelligible to any person who is not authorised to access it, in particular by encrypting personal data. Likewise, the communication to the data subject is not required if the controller has taken subsequent measures which ensure that the high risk for the rights and freedoms of affected data subjects is no longer likely to materialise.	

	Amendment 36		
(44) The controller or the processor should designate a person who would assist the controller or processor to monitor compliance with the provisions adopted pursuant to this Directive. A data protection officer may be appointed jointly by several entities of the competent authority. The data protection officers must be in a position to perform their duties and tasks independently and effectively.	(44) The controller or the processor should designate a person who would assist the controller or processor to monitor ***and demonstrate*** compliance with the provisions adopted pursuant to this Directive. ~~A data protection officer may be appointed jointly by~~ ***Where*** several ~~entities of the competent authority.~~ ***competent authorities are acting under the supervision of a central authority, at least this central authority should designate such data protection officer.*** The data protection officers must be in a position to perform their duties and tasks independently and effectively***, in particular by establishing rules that avoid conflicts of interests with other tasks performed by the data protection officer***.	(44) (…) A person with expert knowledge of data protection law and practices may (…) assist the controller or processor to monitor internal compliance with the provisions adopted pursuant to this Directive. This person may inform and advise the controller or the processor and the employees who are processing personal data of their relevant data protection obligations. A data protection officer may be appointed jointly by several (…) competent authorities or bodies, taking into account of their organisational structure and size. Such data protection officers must be in a position to perform their duties and tasks in an independent (…) manner.	

	Amendment 37		
(45) Member States should ensure that a transfer to a third country only takes place if it is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the controller in the third country or international organisation is an authority competent within the meaning of this Directive. A transfer may take place in cases where the Commission has decided that the third country or international organisation in question ensures an adequate level or protection, or when appropriate safeguards have been adduced.	(45) Member States should ensure that a transfer to a third country only takes place if ~~it~~***that specific transfer*** is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the controller in the third country or international organisation is ~~an~~ ***a public*** authority competent within the meaning of this Directive. A transfer may take place in cases where the Commission has decided that the third country or international organisation in question ensures an adequate level or protection, or when appropriate	(45) Member States should ensure that a transfer to a third country or to an international organisation only takes place if it is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties or the safeguarding against and the prevention of threats to public security, and the controller in the third country or international organisation is an authority competent within the meaning of this Directive. A transfer may take place in cases where the Commission has decided that the third country or international organisation in question ensures an adequate level or protection, or when appropriate safeguards have been adduced or when derogations for specific situations apply.	

	safeguards have been adduced***, or where appropriate safeguards have been adduced by way of a legally binding instrument. Data transferred to competent public authorities in third countries should not be further processed for purposes other than the one they were transferred for***.		
	Amendment 38		
	(45a) Further onward transfers from competent authorities in third countries or international organisations to which personal data have been transferred should only be allowed if the onward transfer is necessary for the same specific purpose as the original transfer and the second recipient is also a competent public authority. Further onward transfers should not be allowed for general law-enforcement purposes. The competent authority that carried out the original transfer should have agreed to the onward transfer.	(45a) Where personal data are transferred from a Member State to third countries or international organisations, such transfer should, in principle, take place only after the Member State from which the data were obtained has given its authorisation to the transfer. The interests of efficient law enforcement cooperation require that where the nature of a threat to the public security of a Member State or a third country or to the essential interests of a Members State is so immediate as to render it impossible to obtain prior authorisation in good time,	

		the competent authority should be able to transfer the relevant personal data to the third country or international organisation concerned without such prior authorisation. Member States should provide that any specific conditions concerning the transfer should be communicated to third countries and/or international organisations.	
(46) The Commission may decide with effect for the entire Union that certain third countries, or a territory or a processing sector within a third country, or an international organisation, offer an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third countries or international organisations which are considered to provide such level of protection. In these cases, transfers of personal data to these countries may take place without needing to obtain any further authorisation.	(46) The Commission may decide with effect for the entire Union that certain third countries, or a territory or a processing sector within a third country, or an international organisation, offer an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third countries or international organisations which are considered to provide such level of protection. In these cases, transfers of personal data to these countries may take place without needing to obtain any further authorisation.	(46) Where the Commission has not adopted a decision in accordance with Article 41 of Regulation (EU) XXX, it may decide with effect for the entire Union that certain third countries, or a territory or one or more specified sectors within a third country, or an international organisation, offer an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third countries or international organisations which are considered to provide such level of protection. In these cases, transfers of personal data to these countries may take place without needing to obtain any (…) specific authorisation.	

(47) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should take into account how the rule of law, access to justice, as well as international human rights norms and standards, in that third country are respected.	(47) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should take into account how the rule of law, access to justice, as well as international human rights norms and standards, in that third country are respected.	(47) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should take into account how a given third country respects the rule of law, access to justice, as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law (…).	

	Amendment 39		
(48) The Commission should equally be able to recognise that a third country, or a territory or a processing sector within a third country, or an international organisation, does not offer an adequate level of data protection. Consequently the transfer of personal data to that third country should be prohibited except when they are based on an international agreement, appropriate safeguards or a derogation. Provision should be made for procedures for consultations between the Commission and such third countries or international organisations. However, such a Commission decision shall be without prejudice to the possibility to undertake transfers on the basis of appropriate safeguards or on the basis of a derogation laid down in the Directive.	(48) The Commission should equally be able to recognise that a third country, or a territory or a processing sector within a third country, or an international organisation, does not offer an adequate level of data protection. Consequently the transfer of personal data to that third country should be prohibited except when they are based on an international agreement, appropriate safeguards or a derogation. Provision should be made for procedures for consultations between the Commission and such third countries or international organisations. However, such a Commission decision shall be without prejudice to the possibility to undertake transfers on the basis of appropriate safeguards ***by means of legally binding instruments*** or on the basis of a derogation laid down in this Directive.	(48) The Commission should equally be able to recognise that a third country, or a territory or a specified sector within a third country, or an international organisation, (…) no longer ensures an adequate level of data protection. Consequently the transfer of personal data to that third country or international organisation should be prohibited unless the requirements of Articles 35-36 are fulfilled. Provision should be made for procedures for consultations between the Commission and such third countries or international organisations.(…) The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation.	

	Amendment 40		
(49) Transfers not based on such an adequacy decision should only be allowed where appropriate safeguards have been adduced in a legally binding instrument, which ensure the protection of the personal data or where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and, based on this assessment, considers that appropriate safeguards with respect to the protection of personal data exist. In cases where no grounds for allowing a transfer exist, derogations should be allowed if necessary in order to protect the vital interests of the data subject or another person, or to safeguard legitimate interests of	(49) Transfers not based on such an adequacy decision should only be allowed where appropriate safeguards have been adduced in a legally binding instrument, which ensure the protection of the personal data ~~or where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and, based on this assessment, considers that appropriate safeguards with respect to the protection of personal data exist. In cases where no grounds for allowing a transfer exist, derogations should be allowed if necessary in order to protect the vital interests of the data subject or another person, or to safeguard legitimate interests of the~~	(49) Transfers not based on such an adequacy decision should only be allowed where appropriate safeguards have been adduced in a legally binding instrument, which ensure the protection of the personal data or where the controller (…) has assessed all the circumstances surrounding the data transfer (…) and, based on this assessment, considers that appropriate safeguards with respect to the protection of personal data exist. Such legally binding instruments could for example be legally binding bilateral agreements which have been concluded by the Member States and implemented in their legal order and may be enforced by their data subjects, ensuring compliance with data protection requirements and the rights of the data subjects, including the right to obtain effective administrative or judicial redress**.** The controller may take into account cooperation agreements concluded between	

the data subject where the law of the Member State transferring the personal data so provides, or where it is essential for the prevention of an immediate and serious threat to the public security of a Member State or a third country, or in individual cases for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, or in individual cases for the establishment, exercise or defence of legal claims.	~~data subject where the law of the Member State transferring the personal data so provides, or where it is essential for the prevention of an immediate and serious threat to the public security of a Member State or a third country, or in individual cases for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, or in individual cases for the establishment, exercise or defence of legal claims~~.	Europol or Eurojust and third countries which allow for the exchange of personal data when carrying out the assessment of all the circumstances surrounding the data transfer. The controller may also take into account that the transfer of personal data will be subject to confidentiality obligations and the principle of specificity, ensuring that the data will not be processed for other purposes than for the purposes of the transfer. In addition the controller should take into account that the personal data will not be used to request, hand down or execute the death penalty or any form of cruel and inhuman treatment. While these conditions could be considered as appropriate safeguards allowing the transfer of data, the controller may require additional safeguards.	

	Amendment 41		
	(49a) In cases where no grounds for allowing a transfer exist, derogations should be allowed if necessary in order to protect the vital interests of the data subject or another person, or to safeguard legitimate interests of the data subject where the law of the Member State transferring the personal data so provides, or where it is essential for the prevention of an immediate and serious threat to the public security of a Member State or a third country, or in individual cases for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, or in individual cases for the establishment, exercise or defence of legal claims.		

	Those derogations should be interpreted restrictively and should not allow frequent, massive and structural transfer of personal data and should not allow wholesale transfer of data which should be limited to data strictly necessary. Moreover, the decision for transfer should be made by a duly authorised person and that transfer must be documented and should be made available to the supervisory authority on request in order to monitor the lawfulness of the transfer.		
		(49aa) Where no adequacy decision or appropriate safeguards exist, a transfer or a category of transfers could only take place in specific situations if necessary in order to protect the vital interests of the data subject or another person, or to safeguard legitimate interests of the data subject where the law of the Member State transferring the personal data so provides, or where it is necessary for the prevention of an immediate and serious threat to the public	

		security of a Member State or a third country, or necessary in an individual case for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties or the safeguarding against and the prevention of public security, or necessary in an individual case for the establishment, exercise or defence of legal claims**.**	
		(49b) Competent authorities of Member States are applying bilateral or multilateral international agreements in force, concluded with third countries in the field of judicial co-operation in criminal matters and police co-operation, for the exchange of relevant information to allow them to perform their legally assigned tasks. In principle, this takes place through or at least with the cooperation of the competent authorities of the concerned third countries. However, in specific individual cases, it may occur that the procedures provided	

		for by the international agreements applicable do not allow to exchange the relevant information in a timely manner, so that competent authorities of Member States have to transfer personal data directly to recipients established in third countries. This may be the case when criminal offences have been committed by means of electronic communication technology like social networks, or where data generated by communication technology are relevant as evidence of the perpetration of a criminal offence or where there is an urgent need to transfer personal data to save the life of a person who is in danger of becoming a victim of a criminal offence. Even if this exchange between competent authorities and recipients established in third countries should only take place in individual and specific cases, this Directive should provide for conditions to regulate such cases. These provisions should not be	

		considered as derogations to any existing bilateral or multilateral international agreements in the field of judicial co-operation in criminal matters and police co-operation. These rules should apply in addition to the other rules of the Directive, in particular those on the lawfulness of processing and of Chapter V.	
(50) When personal data moves across borders it may put at increased risk the ability of individuals to exercise data protection rights to protect themselves from the unlawful use or disclosure of that data. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also	(50) When personal data move across borders it may put at increased risk the ability of individuals to exercise data protection rights to protect themselves from the unlawful use or disclosure of that data. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient	(50) deleted	

be hampered by insufficient preventative or remedial powers, inconsistent legal regimes. Therefore, there is a need to promote closer co-operation among data protection supervisory authorities to help them exchange information with their foreign counterparts.	preventative or remedial powers, inconsistent legal regimes. Therefore, there is a need to promote closer co-operation among data protection supervisory authorities to help them exchange information with their foreign counterparts.		
	Amendment 42		
(51) The establishment of supervisory authorities in Member States, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of their personal data. The supervisory authorities should monitor the application of the provisions pursuant to this Directive and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data. For that purpose, the supervisory authorities should co-operate with each other and the Commission.	(51) The establishment of supervisory authorities in Member States, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of their personal data. The supervisory authorities should monitor the application of the provisions pursuant to this Directive and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data. For that purpose, the supervisory authorities should co-operate with each other ~~and the Commission~~.	(51) The establishment of supervisory authorities in Member States, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of their personal data. The supervisory authorities should monitor the application of the provisions adopted pursuant to this Directive and contribute to their consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data. For that purpose, the supervisory authorities should co-operate with each other and the Commission.	

(52) Member States may entrust a supervisory authority already established in Member States under Regulation (EU)…./2012 with the responsibility for the tasks to be performed by the national supervisory authorities to be established under this Directive.	(52) Member States may entrust a supervisory authority already established in Member States under Regulation (EU) …/2014 with the responsibility for the tasks to be performed by the national supervisory authorities to be established under this Directive.	(52) Member States may entrust a supervisory authority already established (…) under Regulation EU/XXX with the responsibility for the tasks to be performed by the national supervisory authorities to be established under this Directive.	
	Amendment 43		
(53) Member States should be allowed to establish more than one supervisory authority to reflect their constitutional, organisational and administrative structure. Each supervisory authority should be provided with adequate financial and human resources, premises and infrastructure, which are necessary for the effective performance of their tasks, including for the tasks related to mutual assistance and co-operation with other supervisory authorities throughout the Union.	(53) Member States should be allowed to establish more than one supervisory authority to reflect their constitutional, organisational and administrative structure. Each supervisory authority should be provided with adequate financial and human resources, premises and infrastructure, ***including technical capabilities, experience and skills,*** which are necessary for the effective performance of their tasks, including for the tasks related to mutual assistance and co-operation with other supervisory authorities throughout the Union.	(53) Member States should be allowed to establish more than one supervisory authority to reflect their constitutional, organisational and administrative structure. Each supervisory authority should be provided with (…) financial and human resources, premises and infrastructure, which are necessary for the effective performance of their tasks, including for the tasks related to mutual assistance and co-operation with other supervisory authorities throughout the Union.	

		(53a) Supervisory authorities should be subject to independent control or monitoring mechanisms regarding their financial expenditure, provided that this financial control does not affect their independence.	
	Amendment 44		
(54) The general conditions for the members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members should be either appointed by the parliament or the government of the Member State, and include rules on the personal qualification of the members and the position of those members.	(54) The general conditions for the members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members should be either appointed by the parliament or the government***, on the basis of the consultation of the parliament,*** of the Member State, and include rules on the personal qualification of the members and the position of those members.	(54) The general conditions for the member or members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members should be either appointed by the parliament or the government or the head of state of the Member State concerned or by an independent body entrusted by Member State law with the appointment by means of a transparent procedure (…).	

(55) While this Directive applies also to the activities of national courts, the competence of the supervisory authorities should not cover the processing of personal data when they are acting in their judicial capacity, in order to safeguard the independence of judges in the performance of their judicial tasks. However, this exemption should be limited to genuine judicial activities in court cases and not apply to other activities where judges might be involved in accordance with national law.	(55) While this Directive applies also to the activities of national courts, the competence of the supervisory authorities should not cover the processing of personal data when they are acting in their judicial capacity, in order to safeguard the independence of judges in the performance of their judicial tasks. However, this exemption should be limited to genuine judicial activities in court cases and not apply to other activities where judges might be involved in accordance with national law.	(55) While this Directive applies also to the activities of national courts and other judicial authorities, the competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of judges in the performance of their judicial tasks. (…) This exemption should be limited to (…) judicial activities in court cases and not apply to other activities where judges might be involved in accordance with national law. Member States may also provide that the competence of the supervisory authority may not cover the processing of personal data of other independent judicial authorities when acting in their judicial capacity, for example public prosecutors office. In any event, the compliance with the rules of this Directive by the courts and other independent judicial authorities should always be subject to independent supervision in accordance with Article 8 (3) of the Charter of Fundamental Rights of the EU.	

	Amendment 45		
(56) In order to ensure consistent monitoring and enforcement of this Directive throughout the Union, the supervisory authorities should have the same duties and effective powers in each Member State, including powers of investigation, legally binding intervention, decisions and sanctions, particularly in cases of complaints from individuals, and to engage in legal proceedings.	(56) In order to ensure consistent monitoring and enforcement of this Directive throughout the Union, the supervisory authorities should have the same duties and effective powers in each Member State, including ***effective*** powers of investigation, ***power to access all personal data and all information necessary for the performance of each supervisory function, power to access any of the premises of the data controller or the processor including data processing equipment, and*** legally binding intervention, decisions and sanctions, particularly in cases of complaints from individuals, and to engage in legal proceedings.	(56) (…) *Each supervisory authority should deal with complaints lodged by any data subject and should investigate the matter. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject.*	Moved from recital (57)

(57) Each supervisory authority should hear complaints lodged by any data subject and should investigate the matter. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject.	(57) Each supervisory authority should hear complaints lodged by any data subject and should investigate the matter. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject.	(57) *In order to ensure consistent monitoring and enforcement of this Directive throughout the Union, the supervisory authorities should have in each Member State the same* tasks *and effective powers, including* investigative, corrective, and advisory powers. However, their powers should not interfere with specific rules set out for criminal proceedings, including investigation and prosecution of criminal offences**,** or the independence of the judiciary. Without prejudice to the powers of prosecutorial authorities under national law, supervisory authorities should also have the power to bring infringements of this Directive to the attention of the judicial authorities and/or to engage in legal proceedings.	Moved from recital (56)

		The powers of supervisory authorities should be exercised in conformity with appropriate procedural safeguards set out in Union law and Member State law, impartially, fairly and within a reasonable time. In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Directive, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned. Investigative powers as regards access to premises should be exercised in accordance with specific requirements in national law, such as the requirement to obtain a prior judicial authorisation. The adoption of a legally binding decision should be subject to judicial review in the Member State of the supervisory authority that adopted the decision.	

	Amendment 46		
(58) The supervisory authorities should assist one another in performing their duties and provide mutual assistance, so as to ensure the consistent application and enforcement of the provisions adopted pursuant to this Directive.	(58) The supervisory authorities should assist one another in performing their duties and provide mutual assistance, so as to ensure the consistent application and enforcement of the provisions adopted pursuant to this Directive. ***Each supervisory authority should be ready to participate in joint operations. The requested supervisory authority should be obliged to respond in a defined time period to the request.***	(58) The supervisory authorities should assist one another in performing their tasks and provide mutual assistance, so as to ensure the consistent application and enforcement of the provisions adopted pursuant to this Directive.	
	Amendment 47		
(59) The European Data Protection Board established by Regulation (EU)…./2012 should contribute to the consistent application of this Directive throughout the Union, including advising the Commission and promoting the co-operation of the supervisory authorities throughout the Union.	(59) The European Data Protection Board established by Regulation (EU) …/~~2012~~ ***2014*** should contribute to the consistent application of this Directive throughout the Union, including advising the ~~Commission and~~ ***Union institutions,*** promoting the co-operation of the supervisory authorities throughout the Union***, and give its opinion to the Commission in the preparation of delegated and implementing acts based on this Directive***.	(59) The European Data Protection Board established by Regulation EU/XXX should contribute to the consistent application of this Directive throughout the Union, including advising the Commission and promoting the co-operation of the supervisory authorities throughout the Union.	

(60) Every data subject should have the right to lodge a complaint with a supervisory authority in any Member State and have the right to a judicial remedy if they consider that their rights under this Directive are infringed or where the supervisory authority does not act on a complaint or does not act where such action is necessary to protect the rights of the data subject.	(60) Every data subject should have the right to lodge a complaint with a supervisory authority in any Member State and have the right to a judicial remedy if they consider that their rights under this Directive are infringed or where the supervisory authority does not act on a complaint or does not act where such action is necessary to protect the rights of the data subject.	(60) Every data subject should have the right to lodge a complaint with a single supervisory authority (…) and have the right to an effective judicial remedy in accordance with Article 47 of the Charter of Fundamental Rights, if the data subject considers that his or her rights under provisions adopted pursuant to this Directive are infringed or where the supervisory authority 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 competent supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority,	

		intermediate information should be given to the data subject. In order to facilitate the submission of complaints, each supervisory authority should take measures such as providing a complaint submission form which can be completed also electronically, without excluding other means of communication.	

	Amendment 48		
(61) Any body, organisation or association which aims to protects the rights and interests of data subjects in relation to the protection of their data and is constituted according to the law of a Member State should have the right to lodge a complaint or exercise the right to a judicial remedy on behalf of data subjects if duly mandated by them, or to lodge, independently of a data subject's complaint, its own complaint where it considers that a personal data breach has occurred.	(61) Any body, organisation or association ~~which aims to protects the rights and interests of data subjects in relation to the protection of their data~~ ***which acts in the public interest*** and is constituted according to the law of a Member State should have the right to lodge a complaint or exercise the right to a judicial remedy on behalf of data subjects if duly mandated by them, or to lodge, independently of a data subject's complaint, its own complaint where it considers that a personal data breach has occurred.	(61) *Each natural or legal person should have the right to* an effective *judicial remedy* (…) before the competent national court against a *decision of a supervisory authority* which produces legal effects concerning this person. Such a decision concerns in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints. However, this right does not encompass other measures of supervisory authorities which are not legally binding, such as opinions issued by or advice provided by the supervisory authority. *Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established* and should be conducted in accordance with the national law of that Member State. Those courts should exercise full jurisdiction which should include jurisdiction to examine all questions of fact and law relevant to the dispute before it.	Moved from recital (62)

(62) Each natural or legal person should have the right to a judicial remedy against decisions of a supervisory authority concerning them. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established.	(62) Each natural or legal person should have the right to a judicial remedy against decisions of a supervisory authority concerning them. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established.	(62) Where a data subject considers that his or her rights under this Directive are infringed, he or she should have the right to mandate a *body, organisation or association which aims to protect the rights and interests of data subjects in relation to the protection of their data and is constituted according to the law of a Member State*, *(...) to lodge a complaint (...)*on his or her behalf with a supervisory authority or to exercise the right to a judicial remedy (…). The right of representation of data subjects should be without prejudice to national procedural law which may require mandatory representation of data subjects by a lawyer as defined by Directive 77/249/EEC before national courts.	Moved from recital (61)
(63) Member States should ensure that court actions, in order to be effective, allow the rapid adoption of measures to remedy or prevent an infringement of this Directive.	(63) Member States should ensure that court actions, in order to be effective, allow the rapid adoption of measures to remedy or prevent an infringement of this Directive.	(63) deleted	

	Amendment 49		
(64) Any damage which a person may suffer as a result of unlawful processing should be compensated by the controller or processor, who may be exempted from liability if they prove that they are not responsible for the damage, in particular where they establish fault on the part of the data subject or in case of force majeure.	(64) Any damage***, including non pecuniary damage,*** which a person may suffer as a result of unlawful processing should be compensated by the controller or processor, who may be exempted from liability if they prove that they are not responsible for the damage, in particular where they establish fault on the part of the data subject or in case of force majeure.	(64) Any damage which a person may suffer as a result of (...) processing that is not in compliance with the provisions adopted pursuant to this Directive should be compensated by the controller or (…) any other authority competent under national law. The concept of damage should be broadly interpreted in the light of the case law of the Court of Justice of the European Union in a manner which fully reflects the objectives of this Directive. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law. When reference is made to a processing that is unlawful or not in compliance with the provisions adopted pursuant to this Directive it also covers processing that is not in compliance with implementing acts adopted in accordance with this Directive. Data subjects should receive full and effective compensation for the damage they have suffered.	

(65) Penalties should be imposed on any natural or legal person, whether governed by private or public law, that fails to comply with this Directive. Member States should ensure that the penalties are effective, proportionate and dissuasive and must take all measures to implement the penalties.	(65) Penalties should be imposed on any natural or legal person, whether governed by private or public law, that fails to comply with this Directive. Member States should ensure that the penalties are effective, proportionate and dissuasive and must take all measures to implement the penalties.	(65) Penalties should be imposed on any natural or legal person, whether governed by private or public law, that fails to comply with the provisions adopted pursuant to this Directive. Member States should ensure that the penalties are effective, proportionate and dissuasive and must take all measures to implement the penalties.	

	Amendment 50		
	(65a) Transmission of personal data to other authorities or private parties in the Union is prohibited unless the transmission is in compliance with law, and the recipient is established in a Member State, and no legitimate specific interests of the data subject prevent transmission, and the transmission is necessary in a specific case for the controller transmitting the data for either the performance of a task lawfully assigned to it, or the prevention of an immediate and serious danger to public security, or the prevention of serious harm to the rights of individuals. The controller should inform the recipient of the purpose of the processing and the supervisory authority of the transmission. The recipient should also be informed of processing restrictions and ensure that they are met.		

	Amendment 51		
(66) In order to fulfil the objectives of this Directive, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free exchange of personal data by competent authorities within the Union, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission. In particular, delegated acts should be adopted in respect of notifications of a personal data breach to the supervisory authority. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and Council.	(66) In order to fulfil the objectives of this Directive, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free exchange of personal data by competent authorities within the Union, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission. In particular, delegated acts should be adopted ~~in respect of notifications of~~ ***to further specify the criteria and conditions for processing operations requiring a data protection impact assessment; the criteria and requirements of*** a ~~personal~~ data breach ~~to the supervisory authority~~***and as regards the adequate level of protection afforded by a third country, or a territory or a processing sector within that third country, or an international***	(66) deleted	

	organisation. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level***, in particular with the European Data Protection Board***. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and ***to the*** Council.		

	Amendment 52		
(67) In order to ensure uniform conditions for the implementation of this Directive as regards documentation by controllers and processors, security of processing, notably in relation to encryption standards, notification of a personal data breach to the supervisory authority, and the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with 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 the Member States of the Commission's exercise of implementing powers.[5] [5] OJ L 55, 28.2.2011, p. 13.	(67) In order to ensure uniform conditions for the implementation of this Directive as regards ~~documentation by controllers and processors,~~ security of processing, notably in relation to encryption standards~~,~~ ***and*** notification of a personal data breach to the supervisory authority, ~~and the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation,~~ implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with 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 the Member States of the Commission's exercise of implementing powers~~[1].	(67) In order to ensure uniform conditions for the implementation of this Directive, implementing powers should be conferred on the Commission for: (…) the adequate level of protection afforded by a third country or a territory or a specified sector within that third country or an international organisation; the format and procedures for mutual assistance and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board. Those powers should be exercised in accordance with 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 the Member States of the Commission's exercise of implementing powers.[5] [5] OJ L 55, 28.2.2011, p. 13.	

	[1] ***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 the Member States of the Commission's exercise of implementing powers (***OJ L 55, 28.2.2011, p. 13***)***.		
	Amendment 53		
(68) The examination procedure should be used for the adoption of measures as regards documentation by controllers and processors, security of processing, notification of a personal data breach to the supervisory authority, and the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation, given that those acts are of general scope.	(68) The examination procedure should be used for the adoption of measures as regards ~~documentation by controllers and processors,~~ security of processing~~,~~ ***and*** notification of a personal data breach to the supervisory authority, ~~and the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation,~~ given that those acts are of general scope.	(68) The examination procedure should be used for the adoption of (…) implementing acts on the adequate level of protection afforded by a third country or a territory or a specified sector within that third country or an international organisation; the format and procedures for mutual assistance and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, given that those acts are of general scope.	

	Amendment 54		
(69) The Commission should adopt immediately applicable implementing acts where, in duly justified cases relating to a third country or a territory or a processing sector within that third country or an international organisation which does not ensure an adequate level of protection, imperative grounds of urgency so require.	***deleted***	(69) The Commission should adopt immediately applicable implementing acts where, in duly justified cases relating to a third country or a territory or a specified sector within that third country or an international organisation which no longer ensure an adequate level of protection, imperative grounds of urgency so require.	

	Amendment 55		
(70) Since the objectives of this Directive, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free exchange of personal data by competent authorities within the Union, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective.	(70) Since the objectives of this Directive, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of ***their*** personal data and to ensure the free exchange of personal data by competent authorities within the Union, cannot be sufficiently achieved by the Member States ~~and can therefore~~ ***but can rather***, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve ~~that objective~~***those objectives. Member States may provide for higher standards than those established in this Directive***.	(70) Since the objectives of this Directive, namely to protect the fundamental rights and freedoms of data subjects and in particular their right to the protection of personal data and to ensure the free exchange of personal data by competent authorities within the Union, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective.	

(71) Framework Decision 2008/977/JHA should be repealed by this Directive.	(71) Framework Decision 2008/977/JHA should be repealed by this Directive.	(71) Framework Decision 2008/977/JHA should be repealed by this Directive. Processing already under way on the date of the entry into force of this Directive should be brought in conformity with this Directive within the period of three years after which this Directive enters into force. However, where such processing is in compliance with the Union law applicable prior to the entry into force of this Directive, the requirements of this Directive concerning the prior consultation of the supervisory authority should not apply to the processing operations already under way prior to the entry into force of this Directive, given that these requirements, by their very nature, are to be met prior to the processing.	

	Amendment 56		
(72) Specific provisions with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties in acts of the Union which were adopted prior to the date of the adoption of this Directive, regulating the processing of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaties, should remain unaffected. The Commission should evaluate the situation with regard to the relation between this Directive and the acts adopted prior to the date of adoption of this Directive regulating the processing of personal data between Member	(72) Specific provisions with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties in acts of the Union which were adopted prior to the date of the adoption of this Directive, regulating the processing of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaties, should remain unaffected. ***Since Article 8 of the Charter and Article 16 TFEU imply that the fundamental right to the protection of personal data should be ensured in a consistent and homogeneous manner through the Union,*** ~~The~~***the*** Commission should***, within***	(72) Specific provisions <u>of acts of the Union adopted in the field of judicial co-operation in criminal matters and police co-operation</u> (…) which were adopted prior to the date of the adoption of this Directive, regulating the processing of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaties, should remain unaffected, <u>such as, for example, the specific provisions concerning the protection of personal data applied pursuant to Council Decision 2008/615/JHA,[13] or Article 23 of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (2000/C 197/01).[14]</u> The Commission should evaluate the situation with regard to the relation<u>ship</u> between this	

States or the access of designated authorities of Member States to information systems established pursuant to the Treaties, in order to assess the need for alignment of these specific provisions with this Directive.	***two years after the entry into force of this Directive,*** evaluate the situation with regard to the relation between this Directive and the acts adopted prior to the date of adoption of this Directive regulating the processing of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaties, ~~in order to assess the need for alignment of these specific provisions with~~ ***and should present appropriate proposals with a view to ensuring consistent and homogeneous legal rules relating to the processing of personal data by competent authorities or the access of designated authorities of Member States to information systems established pursuant to the Treaties as well as the processing of personal data by Union institutions, bodies, offices and agencies for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties within the scope of*** this Directive.	Directive and the acts adopted prior to the date of adoption of this Directive regulating the processing of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaties, in order to assess the need for alignment of these specific provisions with this Directive. [13]Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6.8.2008, p. 1. [14]Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C 197, 12.7.2000, p. 1.	

	Amendment 57		
(73) In order to ensure a comprehensive and coherent protection of personal data in the Union, international agreements concluded by Member States prior to the entry force of this Directive should be amended in line with this Directive.	(73) In order to ensure a comprehensive and coherent protection of personal data in the Union, international agreements concluded by ***the Union or by the*** Member States prior to the entry force of this Directive should be amended in line with this Directive.	(73) In order to ensure a comprehensive and coherent protection of personal data in the Union, international agreements concluded by Member States prior to the entry force of this Directive (…), and which are in compliance with the relevant Union law applicable prior to the entry into force of this Directive, should remain in force until amended, replaced or repealed.	
(74) This Directive is without prejudice to the rules on combating the sexual abuse and sexual exploitation of children and child pornography as laid down in Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011.[6] **6** OJ L335, 17.12.2011, p. 1.	(74) This Directive is without prejudice to the rules on combating the sexual abuse and sexual exploitation of children and child pornography as laid down in Directive 2011/9**3**/EU of the European Parliament and of the Council.[1] [1]*Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA* (OJ L 335, 17.12.2011, p. 1).	(74) This Directive is without prejudice to the rules on combating the sexual abuse and sexual exploitation of children and child pornography as laid down in Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011. [8]OJ L 335, 17.12.2011, p. 1.	

(75) In accordance with Article 6a of the Protocol on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, as annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, the United Kingdom and Ireland shall not be bound by the rules laid down in this Directive where the United Kingdom and Ireland are not bound by the rules governing the forms of judicial co-operation in criminal matters or police co-operation which require compliance with the provisions laid down on the basis of Article 16 of the Treaty on the Functioning of the European Union.	(75) In accordance with Article 6a of the Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, the United Kingdom and Ireland shall not be bound by the rules laid down in this Directive where the United Kingdom and Ireland are not bound by the rules governing the forms of judicial co-operation in criminal matters or police co-operation which require compliance with the provisions laid down on the basis of Article 16 of the Treaty on the Functioning of the European Union.	(75) In accordance with Article 6a of the Protocol on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, as annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, the United Kingdom and Ireland are not bound by the rules laid down in this Directive which relate to the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the Treaty on the Functioning of the European Union where the United Kingdom and Ireland are not bound by the rules governing the forms of judicial co-operation in criminal matters or police co-operation which require compliance with the provisions laid down on the basis of Article 16 of the Treaty on the Functioning of the European Union.	

	Amendment 58		
(76) In accordance with Articles 2 and 2a of the Protocol on the position of Denmark, as annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark is not bound by this Directive or subject to its application. Given that this Directive builds upon the Schengen acquis, under Title V of Part Three of the Treaty on the Functioning of the European Union, Denmark shall, in accordance with Article 4 of that Protocol, decide within six months after adoption of this Directive whether it will implement it in its national law.	(76) In accordance with Articles 2 and 2a of the Protocol No 22 on the position of Denmark, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark is not bound by this Directive or subject to its application. ~~Given that this Directive builds upon the Schengen acquis, under Title V of Part Three of the Treaty on the Functioning of the European Union, Denmark shall, in accordance with Article 4 of that Protocol, decide within six months after adoption of this Directive whether it will implement it in its national law.~~	(76) In accordance with Articles 2 and 2a of the Protocol on the position of Denmark, as annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark is not bound by the rules laid down in this Directive or subject to their application which relate to the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the Treaty on the Functioning of the European Union. Given that this Directive builds upon the Schengen acquis, under Title V of Part Three of the Treaty on the Functioning of the European Union, Denmark shall, in accordance with Article 4 of that Protocol, decide within six months after adoption of this Directive whether it will implement it in its national law.	

(77) As regards Iceland and Norway, this Directive constitutes a development of provisions of the Schengen acquis, as provided for by the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen acquis.[7] [7] OJ L 176, 10.7.1999, p. 36.	(77) As regards Iceland and Norway, this Directive constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the latters' association with the implementation, application and development of the Schengen *acquis.*[1] [1] OJ L 176, 10.7.1999, p. 36.	(77) As regards Iceland and Norway, this Directive constitutes a development of provisions of the Schengen acquis, as provided for by the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen acquis.[9] [9]OJ L 176, 10.7.1999, p. 36.	
(78) As regards Switzerland, this Directive constitutes a development of provisions of the Schengen acquis, as provided for by the Agreement between the European Union, the European Community and the Swiss Confederation concerning the association of the Swiss Confederation with the implementation, application and development of the Schengen acquis.[7] [7] OJ L 53, 27.2.2008, p. 52.	(78) As regards Switzerland, this Directive constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis.*[1] [1] OJ L 53, 27.2.2008, p. 52.	(78) As regards Switzerland, this Directive constitutes a development of provisions of the Schengen acquis, as provided for by the Agreement between the European Union, the European Community and the Swiss Confederation concerning the association of the Swiss Confederation with the implementation, application and development of the Schengen acquis.[10] [10] OJ L 53, 27.2.2008, p. 52.	

(79) As regards Liechtenstein, this Directive constitutes a development of provisions of the Schengen acquis, as provided for by the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis.[8] [8] OJ L 160 of 18.6.2011, p. 19.	(79) As regards Liechtenstein, this Directive constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis.*[2] **[2]** OJ L 160 of 18.6.2011, p. ***21.***	(79) As regards Liechtenstein, this Directive constitutes a development of provisions of the Schengen acquis, as provided for by the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis.[11] [11] OJ L 160 of 18.6.2011, p. ***21.***	

(80) This Directive respects the fundamental rights and observes the principles recognised in the Charter of Fundamental Rights of the European Union as enshrined in the Treaty, notably the right to respect for private and family life, the right to the protection of personal data, the right to an effective remedy and to a fair trial. Limitations placed on these rights are in accordance with Article 52(1) of the Charter as they are necessary to meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.	(80) This Directive respects the fundamental rights and observes the principles recognised in the Charter as enshrined in the Treaty, notably the right to respect for private and family life, the right to the protection of personal data, the right to an effective remedy and to a fair trial. Limitations placed on these rights are in accordance with Article 52(1) of the Charter as they are necessary to meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.	(80) This Directive respects the fundamental rights and observes the principles recognised in the Charter of Fundamental Rights of the European Union as enshrined in the Treaty, notably the right to respect for private and family life, the right to the protection of personal data, the right to an effective remedy and to a fair trial. Limitations placed on these rights are in accordance with Article 52(1) of the Charter as they are necessary to meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.	

(81) In accordance with the Joint Political Declaration of Member States and the Commission on explanatory documents of 28 September 2011, Member States have undertaken to accompany, in justified cases, the notification of their transposition measures with one or more documents explaining the relationship between the components of a directive and the corresponding parts of national transposition instruments. With regard to this Directive, the legislator considers the transmission of such documents to be justified.	(81) In accordance with the Joint Political Declaration of 28 September 2011 of Member States and the Commission on explanatory documents,[1] Member States have undertaken to accompany, in justified cases, the notification of their transposition measures with one or more documents explaining the relationship between the components of a directive and the corresponding parts of national transposition instruments. With regard to this Directive, the legislator considers the transmission of such documents to be justified. [1] ***OJ C 369, 17.12.2011, p. 14***	(81) In accordance with the Joint Political Declaration of Member States and the Commission on explanatory documents of 28 September 2011, Member States have undertaken to accompany, in justified cases, the notification of their transposition measures with one or more documents explaining the relationship between the components of a directive and the corresponding parts of national transposition instruments. With regard to this Directive, the legislator considers the transmission of such documents to be justified.	

(82) This Directive should not preclude Member States from implementing the exercise of the rights of data subjects on information, access, rectification, erasure and restriction of their personal data processed in the course of criminal proceedings, and their possible restrictions thereto, in national rules on criminal procedure.	(82) This Directive should not preclude Member States from implementing the exercise of the rights of data subjects on information, access, rectification, erasure and restriction of their personal data processed in the course of criminal proceedings, and their possible restrictions thereto, in national rules on criminal procedure,	(82) This Directive should not preclude Member States from implementing the exercise of the rights of data subjects on information, access, rectification, erasure and restriction of their personal data processed in the course of criminal proceedings, and their possible restrictions thereto, in national rules on criminal procedure.	
HAVE ADOPTED THIS DIRECTIVE:	HAVE ADOPTED THIS DIRECTIVE:		

CHAPTER I GENERAL PROVISIONS	CHAPTER I GENERAL PROVISIONS	CHAPTER I GENERAL PROVISIONS	
Article 1	***Article 1***	***Article 1***	
Subject matter and objectives	***Subject matter and objectives***	***Subject matter and objectives***	
	Amendment 59		
1. This Directive lays down the rules relating to the protection of individuals 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	1. This Directive lays down the rules relating to the protection of individuals 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~~ ***and*** the execution of criminal penalties ***and conditions for the free movement of such personal data.***	1. This Directive lays down the rules relating to the protection of individuals 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 or the safeguarding against and the prevention of threats to public security.	

		1a. <u>This Directive shall not preclude Member States from providing higher safeguards than those established in this Directive for the protection of the rights and freedoms of the data subject with regard to the processing of personal data by competent authorities.</u>	Corresponds to EP amendment 59: paragraph 2a
2. In accordance with this Directive, Member States shall:	2. In accordance with this Directive, Member States shall:	2. In accordance with this Directive, Member States shall:	
(a) protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data; and	(a) protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of ***their*** personal data ***and privacy***; and	(a) protect the fundamental rights and freedoms of (…) <u>individuals</u> and in particular their right to the protection of personal data; and	
(b) ensure that the exchange of personal data by competent authorities within the Union is neither restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.	(b) ensure that the exchange of personal data by competent authorities within the Union is neither restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.	(b) ensure that the exchange of personal data by competent authorities within the Union<u>, where such exchange is required by Union or national law</u>**<u>,</u>** is neither restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.	

	2a. This Directive shall not preclude Member States from providing higher safeguards than those established in this Directive.		Council text Article 1(1a)
Article 2	***Article 2***	***Article 2***	
Scope	***Scope***	***Scope***	
1. This Directive applies to the processing of personal data by competent authorities for the purposes referred to in Article 1(1).	1. This Directive applies to the processing of personal data by competent authorities for the purposes referred to in Article 1(1).	1. This Directive applies to the processing of personal data by competent authorities for the purposes set out in Article 1(1).	
2. This Directive applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.	2. This Directive applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.	2. This Directive applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.	
	Amendment 60		
3. This Directive shall not apply to the processing of personal data:	3. This Directive shall not apply to the processing of personal data:	3. This Directive shall not apply to the processing of personal data:	

(a) in the course of an activity which falls outside the scope of Union law, in particular concerning national security;	(a) in the course of an activity which falls outside the scope of Union law~~, in particular concerning national security;~~	(a) in the course of an activity which falls outside the scope of Union law (…);	
(b) by the Union institutions, bodies, offices and agencies.	***deleted***	(b) by the Union institutions, bodies, offices and agencies.	
Article 3	***Article 3***	***Article 3***	
Definitions	***Definitions***	***Definitions***	
	Amendment 61		
For the purposes of this Directive:	For the purposes of this Directive:	For the purposes of this Directive:	

(1) 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifiers or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;	~~(1) 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifiers or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;~~	(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable 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, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.	Merges Article 3(1) and (2)
(2) 'personal data' means any information relating to a data subject;	(2) 'personal data' means any information relating to a***an identified or identifiable natural person (‘***data subject***’)***; ***an identifiable 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, unique identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social or gender identity of that person;***	(2) deleted	Merged with Article 3(1)

	(2a) 'pseudonymous data' means personal data that cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution;		See Article 3 (4a) in Council text
(3) 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;	(3) 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;	(3) 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination**,** restriction, erasure or destruction;	

	(3a) 'profiling' means any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person or to analyse or predict in particular that natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour;		
(4) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;	(4) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;	(4) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;	
		(4a) 'pseudonymisation' means the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person.	

(5) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;	(5) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;	(5) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;	
(6) 'controller' means the competent public authority which alone or jointly with others determines the purposes, conditions and means of the processing of personal data; where the purposes, conditions and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;	(6) 'controller' means the competent public authority which alone or jointly with others determines the purposes~~, conditions~~ and means of the processing of personal data; where the purposes~~, conditions~~ and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;	(6) 'controller' means the competent (…) authority, 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 Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;	

(7) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;	(7) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;	(7) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;	
(8) 'recipient' means a natural or legal person, public authority, agency or any other body to which the personal data are disclosed;	(8) 'recipient' means a natural or legal person, public authority, agency or any other body to which the personal data are disclosed;	(8) 'recipient' means a natural or legal person, public authority, agency or any other body to which the personal data are disclosed, whether a third party or not; however, national authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;	
(9) '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;	(9) '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;	(9) '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;	

(10) 'genetic data' means all data, of whatever type, concerning the characteristics of an individual which are inherited or acquired during early prenatal development;	(10) 'genetic data' means all data, of whatever type, concerning the characteristics of an individual which are inherited or acquired during early prenatal development;	(10) 'genetic data' means all personal data, relating to the genetic characteristics of an individual that have been inherited or acquired (…), which give unique information about the physiology or the health of that individual, resulting in particular from an analysis of a biological sample from the individual in question**;**	
(11) 'biometric data' means any data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data;	(11) 'biometric data' means any ***personal*** data relating to the physical, physiological or behavioural characteristics of an individual which allow his or her unique identification, such as facial images, or dactyloscopic data;	(11) deleted	
(12) ‘data concerning health’ means any information which relates to the physical or mental health of an individual, or to the provision of health services to the individual;	(12) ‘data concerning health’ means any ~~information~~ ***personal data*** which relate to the physical or mental health of an individual, or to the provision of health services to the individual;	(12) 'data concerning health’ means (…) data related to the physical or mental health of an individual, (…) which reveal information about his or her health status;	

		(12a) 'profiling' means any form of automated processing of personal data consisting of using those data to evaluate personal aspects relating to an natural person, in particular to analyse and predict aspects concerning performance at work, economic situation, health, personal preferences, or interests, reliability or behaviour, location or movements;	See EP text Article 3(3a)
(13) 'child' means any person below the age of 18 years;	(13) 'child' means any person below the age of 18 years;	(13) deleted	
(14) 'competent authorities' means any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;	(14) 'competent authorities' means any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;	(14) 'competent authority' means any public authority competent in each Member State for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties or the safeguarding against and the prevention of threats to public security or any body/entity entrusted by national law to perform public duties or exercise public powers for the purposes set out in Article 1(1).	

(15) 'supervisory authority' means a public authority which is established by a Member State in accordance with Article 39.	(15) 'supervisory authority' means a public authority which is established by a Member State in accordance with Article 39.	(15) 'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 39.	
		(16) '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 as well as Interpol.	

CHAPTER II PRINCIPLES	CHAPTER II PRINCIPLES	CHAPTER II PRINCIPLES	
Article 4	***Article 4***	***Article 4***	
Principles relating to personal data processing	***Principles relating to personal data processing***	***Principles relating to personal data processing***	
	Amendment 62		
Member States shall provide that personal data must be:	Member States shall provide that personal data must be:	1. Member States shall provide that personal data must be:	
(a) processed fairly and lawfully;	(a) processed ~~fairly and~~ lawfully***, fairly and in a transparent and verifiable manner in relation to the data subject***;	(a) processed lawfully and fairly;	
(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;	(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;	(b) collected for specified, explicit and legitimate purposes and not (…) processed in a way incompatible with those purposes;	

(c) adequate, relevant, and not excessive in relation to the purposes for which they are processed;	(c) adequate, relevant, and not excessive ***limited to the minimum necessary*** in relation to the purposes for which they are processed; ***they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data;***	(c) adequate, relevant, and not excessive in relation to the purposes for which they are processed;	
(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;	(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;	(d) accurate and, where necessary, kept up to date; (…)	
(e) kept in a form which permits identification of data subjects for no longer than it is necessary for the purposes for which the personal data are processed;	(e) kept in a form which permits identification of data subjects for no longer than it is necessary for the purposes for which the personal data are processed;	(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;	
		(ee) processed in a manner that ensures appropriate security of the personal data.	

(f) processed under the responsibility and liability of the controller, who shall ensure compliance with the provisions adopted pursuant to this Directive.	(f) processed under the responsibility and liability of the controller, who shall ensure ***and be able to demonstrate*** compliance with the provisions adopted pursuant to this Directive;	(f) deleted	
	(fa) processed in a way that effectively allows the data subject to exercise his or her rights as described in Articles 10 to 17;		
	(fb) processed in a way that protects against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;		
	(fc) processed by only those duly authorised staff of the competent authorities who need them for the performance of their tasks.		
		2. Processing by the same or another controller for other purposes set out in Article 1 (1) than the one for which the data are collected shall be permitted in so far as:	

		(a) the controller is authorised to process such personal data for such purpose in accordance with the applicable legal provisions; and (b) processing is necessary and proportionate to that other purpose.	
		3. Processing by the same or another controller may include archiving in the public interest, scientific, statistical or historical use for the purposes set out in Article 1 (1), subject to appropriate safeguards for the rights and freedoms of data subjects.	

		4. The controller shall be responsible for compliance with paragraphs 1, 2 and 3.	
	Article 4a		
	Access to data initially processed for purposes other than those referred to in Article 1(1)		
	Amendment 63		
	1. Member States shall provide that competent authorities may only have access to personal data initially processed for purposes other than those referred to in Article 1(1) if they are specifically authorised by Union or Member State law which must meet the requirements set out in Article 7(1a) and must provide that:		

	(a) access is allowed only to duly authorised staff of the competent authorities in the performance of their tasks where, in a specific case, reasonable grounds give reason to believe that the processing of the personal data will substantially contribute to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;		
	(b) requests for access must be in writing and refer to the legal ground for the request;		
	(c) the written request must be documented; and		
	(d) appropriate safeguards are implemented to ensure the protection of fundamental rights and freedoms in relation to the processing of personal data. Those safeguards shall be without prejudice to and complementary to specific conditions of access to personal data such as judicial authorisation in accordance with Member State law.		

	2. Personal data held by private parties or other public authorities shall only be accessed to investigate or prosecute criminal offences in accordance with necessity and proportionality requirements to be defined by Union law or Member State law, in full compliance with Article 7a.		
	Article 4b		
	Time limits of storage and review		
	Amendment 64		
	1. Member States shall provide that personal data processed pursuant to this Directive shall be deleted by the competent authorities where they are no longer necessary for the purposes for which they were processed.		

	2. Member States shall provide that the competent authorities put mechanisms in place to ensure that time-limits, pursuant to Article 4, are established for the erasure of personal data and for a periodic review of the need for the storage of the data, including fixing storage periods for the different categories of personal data. Procedural measures shall be established to ensure that those time-limits or the periodic review intervals are observed.		

Article 5	*Article 5*	*Article 5*	
Distinction between different categories of data subjects	~~*Distinction between different*~~***Different*** *categories of data subjects*	***Distinction between different categories of data subjects***	
	Amendment 65		
1. Member States shall provide that, as far as possible, the controller makes a clear distinction between personal data of different categories of data subjects, such as:	1. Member States shall provide that~~,~~ ~~as far as possible, the controller makes~~ ***the competent authorities, for the purposes referred to in Article 1(1), may process personal data of the following different categories of data subjects, and the controller shall make*** a clear distinction between ~~personal data of different categories of data subjects, such as~~ ***such categories***:	(1) deleted	
(a) persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence;	(a) persons with regard to whom there are ~~serious~~***reasonable*** grounds for believing that they have committed or are about to commit a criminal offence;	(a) deleted	
(b) persons convicted of a criminal offence;	(b) persons convicted of a ~~criminal offence~~***crime***;	(b) deleted	

(c) victims of a criminal offence, or persons with regard to whom certain facts give reasons for believing that he or she could be the victim of a criminal offence;	(c) victims of a criminal offence, or persons with regard to whom certain facts give reasons for believing that he or she could be the victim of a criminal offence; ***and***	(c) deleted	
(d) third parties to the criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, or a person who can provide information on criminal offences, or a contact or associate to one of the persons mentioned in (a) and (b); and	(d) third parties to the criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, or a person who can provide information on criminal offences, or a contact or associate to one of the persons mentioned in (a) and (b)~~; and.~~	(d) deleted	
(e) persons who do not fall within any of the categories referred to above.	***deleted***	(e) deleted	
	2. Personal data of data subjects other than those referred to under paragraph 1 may only be processed:		

	(a) as long as necessary for the investigation or prosecution of a specific criminal offence in order to assess the relevance of the data for one of the categories indicated in paragraph 1; or		
	(b) when such processing is indispensable for targeted, preventive purposes or for the purposes of criminal analysis, if and as long as this purpose is legitimate, well-defined and specific and the processing is strictly limited to assess the relevance of the data for one of the categories indicated in paragraph 1. This is subject to regular review at least every six months. Any further use is prohibited.		
	3. Member States shall provide that additional limitations and safeguards, according to Member State law, apply to the further processing of personal data relating to data subjects referred to in points (c) and (d) of paragraph 1.		

Article 6	***Article 6***	***Article 6***	
Different degrees of accuracy and reliability of personal data	***Different degrees of accuracy and reliability of personal data***	***Verification of quality of data that are transmitted or made available***	
	Amendment 66		
Member States shall ensure that, as far as possible, the different categories of personal data undergoing processing are distinguished in accordance with their degree of accuracy and reliability.	1. Member States shall ~~ensure~~ ***provide*** that~~, as far as possible, the different categories~~ ***accuracy and reliability*** of personal data undergoing processing are ~~distinguished in accordance with their degree of accuracy and reliability~~ ***ensured***.	Deleted	
Member States shall ensure that, as far as possible, personal data based on facts are distinguished from personal data based on personal assessments.	2. Member States shall ensure that~~,~~ ~~as far as possible,~~ personal data based on facts are distinguished from personal data based on personal assessments***, in accordance with their degree of accuracy and reliability***.	Deleted	

	2a. Member States shall ensure that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. To this end, the competent authorities shall assess the quality of personal data before they are transmitted or made available. As far as possible, in all transmissions of data, available information shall be added which enables the receiving Member State to assess the degree of accuracy, completeness, and reliability of the data, and the extent to which they are up-to-date. Personal data shall not be transmitted without request from a competent authority, in particular data originally held by private parties.	1. Member States shall provide that the competent authorities shall take all reasonable steps to ensure that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. To that end, each competent authority shall as far as practicable verify quality of personal data before they are transmitted or made available. As far as possible, in all transmissions of personal data, necessary information shall be added which enables the receiving competent authority to assess the degree of accuracy, completeness, up-to-datedness and reliability of personal data.	

	2b. If it emerges that incorrect data have been transmitted or data have been transmitted unlawfully, the recipient must be notified without delay. The recipient shall be obliged to rectify the data without delay in accordance with paragraph 1 and Article 15 or to erase them in accordance with Article 16.	2. If it emerges that incorrect personal data have been transmitted or the data have been unlawfully transmitted, the recipient must be notified without delay. In such case the personal data must be rectified, erased or restricted in accordance with Article 15.	
Article 7	***Article 7***	***Article 7***	
Lawfulness of processing	***Lawfulness of processing***	***Lawfulness of processing***	
	Amendment 67		
1. Member States shall provide that the processing of personal data is lawful only if and to the extent that processing is necessary:	***1.*** Member States shall provide that the processing of personal data is lawful only if and to the extent that processing ***is based on Union or Member State law for the purposes set out in Article 1(1) and it*** is necessary:	(…) Member States shall provide that the processing of personal data is lawful only if and to the extent that processing is necessary (…) *for the performance of a task carried out by a competent authority for the purposes set out in Article 1(1)* and is *based on* Union *law* or Member State law (…).	Text moved from Article 7(1) (a)

(a) for the performance of a task carried out by a competent authority, based on law for the purposes set out in Article 1(1); or	(a) for the performance of a task carried out by a competent authority~~, based on law for the purposes set out in Article 1(1)~~; or	deleted	
(b) for compliance with a legal obligation to which the controller is subject; or	***deleted***	(b) deleted	
(c) in order to protect the vital interests of the data subject or of another person; or	(c) in order to protect the vital interests of the data subject or of another person; or	(c) deleted	
(d) for the prevention of an immediate and serious threat to public security.	(d) for the prevention of an immediate and serious threat to public security.	(d) deleted	
	1a. Member State law regulating the processing of personal data within the scope of this Directive shall contain explicit and detailed provisions specifying at least:		
	(a) the objectives of the processing;		
	(b) the personal data to be processed;		
	(c) the specific purposes and means of processing;		

	(d) the appointment of the controller, or of the specific criteria for the appointment of the controller;		
	(e) the categories of duly authorised staff of the competent authorities for the processing of personal data;		
	(f) the procedure to be followed for the processing;		
	(g) the use that may be made of the personal data obtained;		
	(h) limitations on the scope of any discretion conferred on the competent authorities in relation to the processing activities.		

	Article 7a (new)		
	Further processing for incompatible purposes		
	Amendment 68		
	1. Member States shall provide that personal data may only be further processed for another purpose set out in Article 1(1) which is not compatible with the purposes for which the data were initially collected if and to the extent that:		
	(a) the purpose is strictly necessary and proportionate in a democratic society and required by Union or Member State law for a legitimate, well-defined and specific purpose;		
	(b) the processing is strictly limited to a period not exceeding the time needed for the specific data processing operation;		
	(c) any further use for other purposes is prohibited.		

	Prior to any processing, the Member State shall consult the competent national supervisory authority and conduct a data protection impact assessment.		
	2. In addition to the requirements set out in Article 7(1a), Member State law authorising further processing as referred to in paragraph 1 shall contain explicit and detailed provisions specifying at least:		
	(a) the specific purposes and means of that particular processing;		
	(b) that access is allowed only by the duly authorised staff of the competent authorities in the performance of their tasks where in a specific case there are reasonable grounds for believing that the processing of the personal data will contribute substantially to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; and		

	(c) that appropriate safeguards are established to ensure the protection of fundamental rights and freedoms in relation to the processing of personal data.		
	Member States may require that access to the personal data is subject to additional conditions such as judicial authorisation, in accordance with their national law.		
	3. Member States may also allow further processing of personal data for historical, statistical or scientific purposes provided that they establish appropriate safeguards, such as making the data anonymous.		

		Article 7a	
		Specific processing conditions	
		1. Personal data collected by competent authorities for the purposes set out in Article 1(1) shall not be processed for other purposes than those set out in Article 1(1) unless: such processing is authorized by Union law or Member State law. In these cases, Regulation EU/XXX shall apply for this processing unless the processing is carried out in an activity which falls outside the scope of Union law.	
		1a. Where competent authorities are entrusted by Member State law with the performance of tasks other than for the purposes set out in Article 1 (1), Regulation EU/XXX shall apply to the processing for such purposes, including, for archiving in the public interest, scientific, statistical or historical use, unless the processing is carried out in an activity which falls outside the scope of Union law.	

		1b. Member States shall provide that where Union law or the national law applicable to the transmitting competent authority provides specific conditions to the processing of personal data, the transmitting competent authority shall inform the recipient to whom the data are transmitted about such conditions and the requirement to respect them.	
		2. Member States shall provide that the transmitting competent authority does not apply conditions pursuant to paragraph 1b to recipients in other Member States or to agencies, offices and bodies established pursuant to Chapters IV and V of Title V of the Treaty on the Functioning of the European Union other than those applicable to similar transmissions of data within the Member State of the transmitting competent authority.	

Article 8	***Article 8***	***Article 8***	
Processing of special categories of personal data	***Processing of special categories of personal data***	***Processing of special categories of personal data***	
	Amendment 69		
1. Member States shall prohibit the processing of personal data revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, of genetic data or of data concerning health or sex life.	1. Member States shall prohibit the processing of personal data revealing race or ethnic origin, political opinions, religion or ***philosophical*** beliefs, ***sexual orientation or gender identity,*** trade-union membership, of genetic ***and activities, and the processing of biometric*** data or of data concerning health or sex life.	(…)The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of genetic data or of data concerning health or sex life shall only be allowed when strictly necessary and subject to appropriate safeguards for the rights and freedoms of the data subject and only if:	
1. Paragraph 1 shall not apply where:	2. Paragraph 1 shall not apply where:	Deleted	

(a) the processing is authorised by a law providing appropriate safeguards; or	(a) the processing is authorised by a law providing appropriate safeguards ***strictly necessary and proportionate for the performance of a task carried out by the competent authorities for the purposes set out in Article 1(1), on the basis of Union or Member State law which shall provide for specific and suitable measures to safeguard the data subject's legitimate interests, including specific authorisation from a judicial authority, if required by national law***; or	(a) (…) authorised by Union law or Member State law; or;	
(b) the processing is necessary to protect the vital interests of the data subject or of another person; or	(b) the processing is necessary to protect the vital interests of the data subject or of another person; or	(b) (…) to protect the vital interests of the data subject or of another person; or	
(c) the processing relates to data which are manifestly made public by the data subject.	(c) the processing relates to data which are manifestly made public by the data subject***, provided that they are relevant and strictly necessary for the purpose pursued in a specific case***.	(c) the processing relates to data which are manifestly made public by the data subject.	

	Amendment 70		
	Article 8a (new)		
	Processing of genetic data for the purpose of a criminal investigation or a judicial procedure		
	1. Member States shall ensure that genetic data may only be used to establish a genetic link within the framework of adducing evidence, preventing a threat to public security or preventing the commission of a specific criminal offence. Genetic data may not be used to determine other characteristics which may be linked genetically.		

	2. Member States shall provide that genetic data or information derived from their analysis may only be retained as long as necessary for the purposes for which data are processed and where the individual concerned has been convicted of serious offences against the life, integrity or security of persons, subject to strict storage periods to be determined by Member State law.		
	3. Member States shall ensure that genetic data or information derived from their analysis is only stored for longer periods when the genetic data cannot be attributed to an individual, in particular when it is found at the scene of a crime.		

Article 9	*Article 9*	*Article 9*	
Measures based on profiling and automated processing	***Measures based on profiling and automated processing***	***(…) Automated individual decision making (…)***	
	Amendment 71		
1. Member States shall provide that measures which produce an adverse legal effect for the data subject or significantly affect them and which are based solely on automated processing of personal data intended to evaluate certain personal aspects relating to the data subject shall be prohibited unless authorised by a law which also lays down measures to safeguard the data subject's legitimate interests.	1. Member States shall provide that measures which produce ~~an adverse~~ ***a*** legal effect for the data subject or significantly affect him or her and which are ***partially or fully*** based ~~solely~~ on automated processing of personal data intended to evaluate certain personal aspects relating to the data subject shall be prohibited unless authorised by a law which also lays down measures to safeguard the data subject's legitimate interests.	(…) Member States shall provide that a decision based solely on automated processing**,** including, profiling**,** which produces an adverse legal effect for the data subject or significantly affects him or her (…) shall be prohibited unless authorised by Union or Member State 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.	
2. Automated processing of personal data intended to evaluate certain personal aspects relating to the data subject shall not be based solely on special categories of personal data referred to in Article 8.	2. Automated processing of personal data intended to evaluate certain personal aspects relating to the data subject shall not be based solely on special categories of personal data referred to in Article 8.	2. deleted	

	2a. Automated processing of personal data intended to single out a data subject without an initial suspicion that the data subject might have committed or will be committing a criminal offence shall only be lawful if and to the extent that it is strictly necessary for the investigation of a serious criminal offence or the prevention of a clear and imminent danger, established on factual indications, to public security, the existence of the State, or the life of persons.		
	2b. Profiling that, whether intentionally or otherwise, has the effect of discriminating against individuals on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union membership, gender or sexual orientation, or that, whether intentionally or otherwise, results in measures which have such effect, shall be prohibited in all cases.		

	Amendment 72		
	Article 9a		
	General principles for the rights of the data subject		
	1. Member States shall ensure that the basis of data protection is clear and with unambiguous rights for the data subject which shall be respected by the data controller. The provisions of this Directive aim to strengthen, clarify, guarantee and where appropriate, codify those rights.		

	2. Member States shall ensure that such rights include, inter alia, the provision of clear and easily understandable information regarding the processing of the data subject's personal data, the right of access, rectification and erasure of his or her data, the right to obtain data, the right to lodge a complaint with the competent data protection authority and to bring legal proceedings as well as the right to compensation and damages resulting from an unlawful processing operation. Such rights shall in general be exercised free of charge. The data controller shall respond to requests from the data subject within a reasonable period of time.		

CHAPTER III RIGHTS OF THE DATA SUBJECT	CHAPTER III RIGHTS OF THE DATA SUBJECT	CHAPTER III RIGHTS OF THE DATA SUBJECT	
Article 10	***Article 10***	***Article 10***	
Modalities for exercising the rights of the data subject	***Modalities for exercising the rights of the data subject***	***Communication and modalities for exercising the rights of the data subject***	
	Amendment 73		
1. Member States shall provide that the controller takes all reasonable steps to have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of the data subjects' rights.	1. Member States shall provide that the controller ~~takes all reasonable steps to have~~ ***has concise,*** transparent***, clear*** and easily accessible policies with regard to the processing of personal data and for the exercise of the data ~~subjects'~~ ***subject's*** rights.	1. deleted	Merged with Article 10(2)

2. Member States shall provide that any information and any communication relating to the processing of personal data are to be provided by the controller to the data subject in an intelligible form, using clear and plain language.	2. Member States shall provide that any information and any communication relating to the processing of personal data are to be provided by the controller to the data subject in an intelligible form, using clear and plain language***, in particular where that information is addressed specifically to a child***.	2. *Member States shall provide that the controller takes all reasonable steps* to provide any information referred to in Article 10a (...) and any communication under Articles 12 and 15 and 29 relating to the processing of personal data to the data subject in an intelligible and easily accessible form, using clear and plain language. The information shall be provided by any appropriate means, including electronically. As a general rule the controller shall provide the information in the same form as the request.	First part moved from Article 10(1)
3. Member States shall provide that the controller takes all reasonable steps to establish procedures for providing the information referred to in Article 11 and for the exercise of the rights of data subjects referred to in Articles 12 to 17.	3. Member States shall provide that the controller ~~takes all reasonable steps to establish~~ ***establishes*** procedures for providing the information referred to in Article 11 and for the exercise of the rights of ***the*** data ~~subjects~~ ***subject*** referred to in Articles 12 to 17. ***Where personal data are processed by automated means, the controller shall provide means for requests to be made electronically.***	3. Member States shall provide that the controller takes all reasonable steps (...) to facilitate the exercise of data subject rights under Articles 12 and 15.	

4. Member States shall provide that the controller informs the data subject about the follow-up given to their request without undue delay.	4. Member States shall provide that the controller informs the data subject about the follow-up given to ~~their~~ ***his or her*** request without ~~undue~~ delay***, and in any event at the latest within one month of receipt of the request. The information shall be given in writing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form***.	4. (…)	
5. Member States shall provide that the information and any action taken by the controller following a request referred to in paragraphs 3 and 4 are free of charge. Where requests are vexatious, in particular because of their repetitive character, or the size or volume of the request, the controller may charge a fee for providing the information or taking the action requested, or the controller may not take the action requested. In that case, the controller shall bear the burden of proving the vexatious character of the request.	5. Member States shall provide that the information and any action taken by the controller following a request referred to in paragraphs 3 and 4 are free of charge. Where requests are ~~vexatious~~ ***manifestly excessive***, in particular because of their repetitive character, ~~or the size or volume of the request,~~ the controller may charge a ***reasonable*** fee***, taking into account the administrative costs,*** for providing the information or taking the action requested~~, or the controller may not take the action requested~~. In that case, the controller shall bear the	5. Member States shall provide that the information <u>provided under Article 10a</u> (...) and any <u>communication under Articles 12, 15 and 29 shall be provided</u> (…) free of charge. Where requests are <u>manifestly unfounded or excessive</u>, in particular because of their repetitive character (…), the controller may <u>refuse to act on the request.</u> In that case, the controller shall bear the burden of demonstrating <u>the manifestly unfounded or excessive</u> character of the request.	

	burden of proving the ~~vexatious~~ ***manifestly excessive*** character of the request.		
	5a. Member States may provide that the data subject may assert his or her rights directly against the controller or through the intermediary of the competent national supervisory authority. Where the supervisory authority has acted at the request of the data subject, the supervisory authority shall inform the data subject of the verifications carried out.		
		5a. Where the controller has reasonable doubts concerning the identity of the individual making the request referred to in Articles 12 and 15, the controller may request the provision of additional information necessary to confirm the identity of the data subject.	

Article 10a	***Article 10a***	***Article 10a***	
Information to the data subject	***Information to the data subject***	***Information to the data subject***	
		1. Member States shall provide that the controller makes available to data subjects at least the following information: (a) the identity and the contact details of the controller; the controller shall also include the contact details of the data protection officer if any; (b) the purposes of the processing for which the personal data are intended; (c) the right to lodge a complaint with a supervisory authority.	See Article 11(1) (a), (b) and (e) of COM proposal
		2. Member States shall provide by law that the controller gives to the data subject information in addition to those referred to in paragraph 1, where this is necessary in a specific case and in order to enable the exercise of his or her rights, in particular where the data are collected without the knowledge of the individual.	

		3. Member States may adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject pursuant to paragraph 2 to the extent that, and as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the individual concerned: (a) to avoid obstructing official or legal inquiries, investigations or procedures; (b) to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties; (c) to safeguard public security; (d) to safeguard national security; (e) to safeguard the rights and freedoms of others.	See Article 11(4) of COM proposal

Article 11	*Article 11*	*Article 11*	
Information to the data subject	***Information to the data subject***	***Information to be provided where the data are collected from the data subject***	
	Amendment 74		
1. Where personal data relating to a data subject are collected, Member States shall ensure that the controller takes all appropriate measures to provide the data subject with at least the following information:	1. Where personal data relating to a data subject are collected, Member States shall ensure that the controller ~~takes all appropriate measures to provide~~ ***provides*** the data subject with at least the following information:	1. deleted	See Article 10a
(a) the identity and the contact details of the controller and of the data protection officer;	(a) the identity and the contact details of the controller and of the data protection officer;	(a) deleted	
(b) the purposes of the processing for which the personal data are intended;	(b) ***the legal basis and*** the purposes of the processing for which the personal data are intended;	(b) deleted	
(c) the period for which the personal data will be stored;	(c) the period for which the personal data will be stored;	(c) deleted	

(d) the existence of the right to request from the controller access to and rectification, erasure or restriction of processing of the personal data concerning the data subject;	(d) the existence of the right to request from the controller access to and rectification, erasure or restriction of processing of the personal data concerning the data subject;	(d) deleted	
(e) the right to lodge a complaint to the supervisory authority referred to in Article 39 and its contact details;	(e) the right to lodge a complaint with the supervisory authority referred to in Article 39 and its contact details;	(e) deleted	
(f) the recipients or categories of recipients of the personal data, including in third countries or international organisations;	(f) the recipients ~~or categories of recipients~~ of the personal data, including in third countries or international organisations, ***and who is authorised to access this data under the laws of that third country or the rules of that international organisation, the existence or absence of an adequacy decision by the Commission or in case of transfers referred to in Article 35 or 36, the means to obtain a copy of the appropriate safeguards used for the transfer***;	(f) deleted	

	(fa) where the controller processes personal data as described in Article 9(1), information about the existence of processing for a measure of the kind referred to in Article 9(1) and the intended effects of such processing on the data subject, information about the logic used in the profiling and the right to obtain human assessment;		
	(fb) information regarding security measures taken to protect personal data;		
(g) any further information in so far as such further information is necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are processed.	(g) any further information in so far as such further information is necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are processed.	(g) deleted	

2. Where the personal data are collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, whether the provision of personal data is obligatory or voluntary, as well as the possible consequences of failure to provide such data.	2. Where the personal data are collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, whether the provision of personal data is mandatory or optional, as well as the possible consequences of failure to provide such data.	(2) deleted	
3. The controller shall provide the information referred to in paragraph 1:	3. The controller shall provide the information referred to in paragraph 1:	3. deleted	
(a) at the time when the personal data are obtained from the data subject, or	(a) at the time when the personal data are obtained from the data subject, or	(a) deleted	
(b) where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection having regard to the specific circumstances in which the data are processed.	(b) where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection having regard to the specific circumstances in which the data are processed.	(b) deleted	

4. Member States may adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject to the extent that, and as long as, such partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the person concerned:	4. Member States may adopt legislative measures delaying, ***or*** restricting or omitting the provision of the information to the data subject***, in a specific case,*** to the extent that, and as long as, such partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the ***fundamental rights and the*** legitimate interests of the person concerned:	4. deleted	
(a) to avoid obstructing official or legal inquiries, investigations or procedures ;	(a) to avoid obstructing official or legal inquiries, investigations or procedures ;	(a) deleted	
(b) to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or for the execution of criminal penalties;	(b) to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or for the execution of criminal penalties;	(b) deleted	
(c) to protect public security;	(c) to protect public security;	(c) deleted	
(d) to protect national security;	(d) to protect national security;	(d) deleted	

(e) to protect the rights and freedoms of others.	(e) to protect the rights and freedoms of others.	(e) deleted	
5. Member States may determine categories of data processing which may wholly or partly fall under the exemptions of paragraph 4.	5. ***Member States shall provide that the controller shall assess, in each specific case, by means of a concrete and individual examination, whether a partial or complete restriction for one of the reasons referred to in paragraph 4 applies.*** Member States may ***by law also*** determine categories of data processing which may wholly or partly fall under the exemptions ***under points (a), (b), (c) and (d)*** of paragraph 4.	5. deleted	

Article 12	*Article 12*	*Article 12*	
Right of access for the data subject	***Right of access for the data subject***	***Right of access for the data subject***	
	Amendment 75		
1. Member States shall provide for the right of the data subject to obtain from the controller confirmation as to whether or not personal data relating to them are being processed. Where such personal data are being processed, the controller shall provide the following information:	1. Member States shall provide for the right of the data subject to obtain from the controller confirmation as to whether or not personal data relating to ~~them~~ ***him or her*** are being processed. Where such personal data are being processed, the controller shall provide the following information***, if it has not already been provided***:	1. Subject to Article 13, Member States shall provide for the right of the data subject to obtain from the controller at reasonable intervals and free of charge confirmation as to whether or not personal data concerning him or her are being processed and where such personal data are being processed to obtain access to such data and the following information by appropriate means**:**	
	(- a) communication of the personal data undergoing processing and of any available information as to their source, and if applicable, intelligible information about the logic involved in any automated processing;		

	(- aa) the significance and envisaged consequences of such processing, at least in the case of the measures referred to in Article 9;		
(a) the purposes of the processing;	(a) the purposes of the processing ***as well as the legal basis for the processing***;	(a) the purposes of the processing;	
(b) the categories of personal data concerned;	(b) the categories of personal data concerned;	(b) deleted	
(c) the recipients or categories of recipients to whom the personal data have been disclosed, in particular the recipients in third countries;	(c) the recipients ~~or categories of recipients~~ to whom the personal data have been disclosed, in particular the recipients in third countries;	(c) the recipients or categories of recipients to whom the personal data have been disclosed, in particular the recipients in third countries or international organisations;	
(d) the period for which the personal data will be stored;	(d) the period for which the personal data will be stored;	(d) the envisaged period for which the personal data will be stored or the rules applicable to calculating this period;	
(e) the existence of the right to request from the controller rectification, erasure or restriction of processing of personal data concerning the data subject;	(e) the existence of the right to request from the controller rectification, erasure or restriction of processing of personal data concerning the data subject;	(e) the existence of the right to request from the controller rectification, erasure or restriction of processing of personal data concerning the data subject;	

(f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;	(f) the right to lodge a complaint with the supervisory authority and the contact details of the supervisory authority;	(f) the right to lodge a complaint with a supervisory authority (…);	
(g) communication of the personal data undergoing processing and of any available information as to their source.	***deleted***	(g) communication of the personal data undergoing processing and, where necessary, of any available information as to their source.	
2. Member States shall provide for the right of the data subject to obtain from the controller a copy of the personal data undergoing processing.	2. Member States shall provide for the right of the data subject to obtain from the controller a copy of the personal data undergoing processing. ***Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.***	2. deleted	

Article 13	*Article 13*	*Article 13*	
Limitations to the right of access	***Limitations to the right of access***	***Limitations to the right of access***	
	Amendment 76		
1. Member States may adopt legislative measures restricting, wholly or partly, the data subject's right of access to the extent that such partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the person concerned:	1. Member States may adopt legislative measures restricting, wholly or partly, ***depending on the specific case,*** the data subject's right of access to the extent ***and for the period*** that such partial or complete restriction constitutes a ***strictly*** necessary and proportionate measure in a democratic society with due regard for the ***fundamental rights and the*** legitimate interests of the person concerned:	1. Member States may adopt legislative measures restricting, wholly or partly, the data subject's right of access to the extent that such partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the individual concerned:	
(a) to avoid obstructing official or legal inquiries, investigations or procedures;	(a) to avoid obstructing official or legal inquiries, investigations or procedures;	(a) to avoid obstructing official or legal inquiries, investigations or procedures;	

(b) to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or the execution of criminal penalties;	(b) to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or the execution of criminal penalties;	(b) to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;	
(c) to protect public security;	(c) to protect public security;	(c) to safeguard public security;	
(d) to protect national security;	(d) to protect national security;	(d) to safeguard national security;	
(e) to protect the rights and freedoms of others.	(e) to protect the rights and freedoms of others.	(e) to safeguard the rights and freedoms of others.	
2. Member States may determine by law categories of data processing which may wholly or partly fall under the exemptions of paragraph 1.	2. ***Member States shall provide that the controller assesses, in each specific case by means of a concrete and individual examination whether a partial or complete restriction for one of the reasons referred to in paragraph 1 applies.*** Member States may ***also*** determine by law categories of data processing which may wholly or partly fall under the exemptions ***under points (a) to (d)*** of paragraph 1.	2. deleted	

3. In cases referred to in paragraphs 1 and 2, Member States shall provide that the controller informs the data subject in writing on any refusal or restriction of access, on the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy. The information on factual or legal reasons on which the decision is based may be omitted where the provision of such information would undermine a purpose under paragraph 1.	3. In cases referred to in paragraphs 1 and 2, Member States shall provide that the controller informs the data subject***, without undue delay,*** in writing on any refusal or restriction of access, on the ~~reasons~~ ***reasoned justification*** for the refusal and on the possibilities of lodging a complaint with the supervisory authority and seeking a judicial remedy. The information on factual or legal reasons on which the decision is based may be omitted where the provision of such information would undermine a purpose under paragraph 1.	3. In cases referred to in paragraph 1 (...), Member States shall provide that the controller informs the data subject in writing of any refusal or restriction of access, and of the reasons for the refusal or the restriction. This shall not apply where the provision of such information would undermine a purpose under paragraph 1. Member States shall provide that the controller informs the data subject of the possibilities of lodging a complaint with a supervisory authority or seeking a judicial remedy.	
4. Member States shall ensure that the controller documents the grounds for omitting the communication of the factual or legal reasons on which the decision is based.	4. Member States shall ensure that the controller documents ***the assessment referred to in paragraph 2 as well as*** the grounds for ~~omitting~~ ***restricting*** the communication of the factual or legal reasons on which the decision is based. ***That information shall be made available to the national supervisory authorities.***	4. Member States shall ensure that the controller documents (…) the factual or legal reasons on which the decision is based.	

Article 14	*Article 14*	*Article 14*	
Modalities for exercising the right of access	***Modalities for exercising the right of access***	***Additional modalities for exercising the right of access***	
	Amendment 77		
1. Member States shall provide for the right of the data subject to request, in particular in cases referred to in Article 13, that the supervisory authority checks the lawfulness of the processing.	1. Member States shall provide for the right of the data subject to request, ***at all times,*** in particular in cases referred to in ~~Article 13~~***Articles 12 and 13***, that the supervisory authority checks the lawfulness of the processing.	1. deleted	
2. Member State shall provide that the controller informs the data subject of the right to request the intervention of the supervisory authority pursuant to paragraph 1.	2. Member ~~State~~ ***States*** shall provide that the controller informs the data subject of the right to request the intervention of the supervisory authority pursuant to paragraph 1.	2. deleted	

3. When the right referred to in paragraph 1 is exercised, the supervisory authority shall inform the data subject at least that all necessary verifications by the supervisory authority have taken place, and of the result as regards the lawfulness of the processing in question.	3. When the right referred to in paragraph 1 is exercised, the supervisory authority shall inform the data subject at least that all necessary verifications by the supervisory authority have taken place, and of the result as regards the lawfulness of the processing in question. ***The supervisory authority shall also inform the data subject of his or her right to seek a judicial remedy.***	3. deleted	
	3a. Member States may provide that the data subject may assert this right directly against the controller or through the intermediary of the competent national supervisory authority.		
	3b. Member States shall ensure that there are reasonable time limits for the controller to respond to requests of the data subject regarding the exercise of his or her right of access.		

Article 15	***Article 15***	***Article 15***	
Right to rectification	*Right to rectification* ***and completion***	***Right to rectification, erasure and restriction of processing***	
	Amendment 78		
1. Member States shall provide for the right of the data subject to obtain from the controller the rectification of personal data relating to them which are inaccurate. The data subject shall have the right to obtain completion of incomplete personal data, in particular by way of a corrective statement.	1. Member States shall provide for the right of the data subject to obtain from the controller the rectification ***or the completion*** of personal data relating to ~~them~~ ***him or her*** which are inaccurate~~. The data subject shall have the right to obtain completion of incomplete personal data~~ ***or incomplete***, in particular by way of a ***completing or*** corrective statement.	1. Member States shall provide for the right of the data subject to obtain from the controller without undue delay the rectification of personal data relating to him or her which are inaccurate. Having regard to the purpose of the processing concerned, Member States shall provide that the data subject has the right to obtain completion of incomplete personal data, including by means of providing a supplementary statement.	

		1a. Member States shall provide for the obligation of the controller to erase personal data without undue delay and of the right of the data subject to obtain from the controller the erasure of personal data concerning him or her without undue delay where the processing does not comply with the provisions adopted pursuant to Articles 4, 7 and 8 of this Directive, or where the data have to be erased for compliance with a legal obligation to which the controller is subject.	
		1b. If the accuracy of an item of personal data is contested by the data subject and its accuracy or inaccuracy cannot be ascertained, restriction of the processing of that data item may take place.	

2. Member States shall provide that the controller informs the data subject in writing on any refusal of rectification, on the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.	2. Member States shall provide that the controller informs the data subject in writing, ~~on~~***, with a reasoned justification, of*** any refusal of rectification ***or completion***, on the reasons for the refusal and on the possibilities of lodging a complaint with the supervisory authority and seeking a judicial remedy.	2. Member States shall provide that the controller informs the data subject in writing of any refusal of rectification, erasure or restriction of the processing, and of the reasons for the refusal. (…) Member States may adopt legislative measures restricting, 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 legitimate interests of the individual concerned in order: (a) to avoid obstructing official or legal inquiries, investigations or procedures; (b) to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties; (c) to safeguard public security; (d) to safeguard national security;	

		(e) to safeguard the rights and freedoms of others. Member States shall provide that the controller informs the data subject (…) of the possibilities of lodging a complaint with a supervisory authority or seeking a judicial remedy.	
	2a. Member States shall provide that the controller shall communicate any rectification carried out to each recipient to whom the data have been disclosed, unless to do so proves impossible or involves a disproportionate effort.		
	2b. Member States shall provide that the controller communicates the rectification of inaccurate personal data to the third party from which the inaccurate personal data originate.		
	2c. Member States shall provide that the data subject may assert this right also through the intermediary of the competent national supervisory authority.		

		3. Member States shall provide that in the cases referred to in paragraphs 1, 1a and 1b the controller shall notify the recipients and that the recipients shall rectify, erase or restrict the processing of the personal data under their responsibility.	
Article 15a	***Article 15a***	***Article 15a***	
		Exercise of rights by the data subject and verification by the supervisory authority	
		1. In cases referred to in Article 13 (3) and Article 15 (2) Member States may adopt measures providing that the rights of the data subject may also be exercised through the competent supervisory authority.	
		2. When the right referred to in paragraph 1 is exercised, the supervisory authority shall inform the data subject at least that all necessary verifications or a review by the supervisory authority have taken place.	

Article 16	***Article 16***	***Article 16***	
Right to erasure	***Right to erasure***	***Right to erasure***	
	Amendment 79		
1. Member States shall provide for the right of the data subject to obtain from the controller the erasure of personal data relating to them where the processing does not comply with the provisions adopted pursuant to Articles 4 (a) to (e), 7 and 8 of this Directive.	1. Member States shall provide for the right of the data subject to obtain from the controller the erasure of personal data relating to ~~them~~ ***him or her*** where the processing does not comply with the provisions adopted pursuant to Articles 4 ~~(a) to (e)~~, ~~7 and 8~~***, 6 and 7 to 8*** of this Directive.	1. deleted	
2. The controller shall carry out the erasure without delay.	2. The controller shall carry out the erasure without delay. ***The controller shall also abstain from further dissemination of such data.***	2. deleted	
3. Instead of erasure, the controller shall mark the personal data where:	3. Instead of erasure, the controller shall ~~mark~~ ***restrict the processing of*** the personal data where:	3. deleted	
(a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data;	(a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data;	(a) deleted	

(b) the personal data have to be maintained for purposes of proof;	(b) the personal data have to be maintained for purposes of proof; ***or for the protection of vital interests of the data subject or another person.***	(b) deleted	
c) the data subject opposes their erasure and requests the restriction of their use instead.	***deleted***	(c) deleted	
	3a. Where processing of personal data is restricted pursuant to paragraph 3, the controller shall inform the data subject before lifting the restriction on processing.		
4. Member States shall provide that the controller informs the data subject in writing of any refusal of erasure or marking of the processing, the reasons for the refusal and the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.	4. Member States shall provide that the controller informs the data subject in writing, ***with a reasoned justification,*** of any refusal of erasure or ~~marking~~ ***restriction*** of the processing, ~~the~~ ***on*** reasons for the refusal and ***on*** the possibilities of lodging a complaint with the supervisory authority and seeking a judicial remedy.	4. deleted	
	4a. Member States shall provide that the controller notifies recipients to whom those data have been sent of any erasure or		

	restriction made pursuant to paragraph 1, unless to do so proves impossible or involves a disproportionate effort. The controller shall inform the data subject about those third parties.		
	4b. Member States may provide that the data subject may assert this right directly against the controller or through the intermediary of the competent national supervisory authority.		
Article 17	***Article 17***	***Article 17***	
Rights of the data subject in criminal investigations and proceedings	***Rights of the data subject in criminal investigations and proceedings***	***Rights of the data subject in criminal investigations and proceedings***	
Member States may provide that the rights of information, access, rectification, erasure and restriction of processing referred to in Articles 11 to 16 are carried out in accordance with national rules on judicial proceedings where the personal data are contained in a judicial decision or record processed in the course of criminal investigations and proceedings.	Member States may provide that the rights of information, access, rectification, erasure and restriction of processing referred to in Articles 11 to 16 are carried out in accordance with national rules on judicial proceedings where the personal data are contained in a judicial decision or record processed in the course of criminal investigations and proceedings.	Member States may provide that the exercise of the rights (…) referred to in Articles 10a, 12 and 15 is carried out in accordance with national law where the personal data are contained in a judicial decision or record or case file processed in the course of criminal investigations and proceedings.	

CHAPTER IV CONTROLLER AND PROCESSOR	CHAPTER IV CONTROLLER AND PROCESSOR	CHAPTER IV CONTROLLER AND PROCESSOR	
SECTION 1 **GENERAL OBLIGATIONS**	**SECTION 1** **GENERAL OBLIGATIONS**	**SECTION 1** **GENERAL OBLIGATIONS**	
Article 18	***Article 18***	***Article 18***	
Responsibility of the controller	***Responsibility of the controller***	***Obligations of the controller***	
	Amendment 80		
1. Member States shall provide that the controller adopts policies and implements appropriate measures to ensure that the processing of personal data is performed in compliance with the provisions adopted pursuant to this Directive.	1. Member States shall provide that the controller adopts policies and implements appropriate measures to ensure ***and be able to demonstrate, in a transparent manner, for each processing operation,*** that the processing of personal data is performed in compliance with the provisions adopted pursuant to this Directive***, both at the time of the determination of the means for processing and at the time of the processing itself***.	1. Member States shall provide that, taking into account the nature, scope, context and purposes of the processing as well as the likelihood and severity of risk for the rights and freedoms of individuals, the controller (…) implements appropriate measures (…) and is able to demonstrate that the processing of personal data is performed in compliance with the provisions adopted pursuant to this Directive.	

		1a. Where proportionate in relation to the processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller, which specify the application of the national data protection rules implementing this Directive.	
2. The measures referred to in paragraph 1 shall in particular include:	2. The measures referred to in paragraph 1 shall in particular include:	2. deleted	
(a) keeping the documentation referred to in Article 23;	(a) keeping the documentation referred to in Article 23;	(a) deleted	
	(aa) performing a data protection impact assessment pursuant to Article 25a;		
(b) complying with the requirements for prior consultation pursuant to Article 26;	(b) complying with the requirements for prior consultation pursuant to Article 26;	(b) deleted	
(c) implementing the data security requirements laid down in Article 27;	(c) implementing the data security requirements laid down in Article 27;	(c) deleted	

(d) designating a data protection officer pursuant to Article 30.	(d) designating a data protection officer pursuant to Article 30~~.~~***;***	(d) deleted	
	(da) drawing up and implementing specific safeguards in respect of the treatment of personal data relating to children, where appropriate.		
3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraph 1 of this Article. If proportionate, this verification shall be carried out by independent internal or external auditors.	3. The controller shall implement mechanisms to ensure the verification of the ***adequacy and*** effectiveness of the measures referred to in paragraph 1 of this Article. If proportionate, this verification shall be carried out by independent internal or external auditors.	3. deleted	

Article 19	*Article 19*	*Article 19*	
Data protection by design and by default	***Data protection by design and by default***	***Data protection by design and by default***	
	Amendment 81		
1. Member States shall provide that, having regard to the state of the art and the cost of implementation, the controller shall implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of provisions adopted pursuant to this Directive and ensure the protection of the rights of the data subject.	1. Member States shall provide that, having regard to the state of the art ~~and the cost of implementation~~, ***current technical knowledge, international best practices and the risks represented by the data processing,*** the controller ***and the processor if any*** shall***, both at the time of the determination of the purposes and means for processing and at the time of the processing itself,*** implement appropriate ***and proportionate*** technical and organisational measures and procedures in such a way that the processing will meet the requirements of provisions adopted pursuant to this Directive and ensure the protection of the rights of the data subject***, in particular with regard to the principles laid down in Article 4. Data protection by design shall have particular regard***	1. Having regard to available technology and the cost of implemention and taking into account the nature, scope, context and purposes of the processing as well as the likelihood and severity of the risks for rights and freedoms of individuals, Member States shall provide that, the controller shall implement (…) technical and organisational measures (…) appropriate to the processing activity being carried out and its objectives, such as pseudonymisation, in such a way that the processing will meet the requirements of provisions adopted pursuant to this Directive and protect the rights of data subjects.	

	to the entire lifecycle management of personal data from collection to processing to deletion, systematically focusing on comprehensive procedural safeguards regarding the accuracy, confidentiality, integrity, physical security and deletion of personal data. Where the controller has carried out a data protection impact assessment pursuant to Article 25a, the results shall be taken into account when developing those measures and procedures.		

2. The controller shall implement mechanisms for ensuring that, by default, only those personal data which are necessary for the purposes of the processing are processed.	2. The controller shall ~~implement mechanisms for ensuring~~ ***ensure*** that, by default, only those personal data which are necessary ~~for the purposes of the processing are processed~~***for each specific purpose of the processing and are especially not collected, retained or disseminated beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals and that data subjects are able to control the distribution of their personal data***.	2. Member States shall provide that the controller shall implement appropriate measures, in particular for automated processing, for ensuring that, by default, only (...) personal data which are necessary for each specific purpose of the processing are processed; this applies to the amount of data collected, the extent of their processing, the period of their storage and their accessibility.	

Article 20	*Article 20*	*Article 20*	
Joint controllers	***Joint controllers***	***Joint controllers***	
	Amendment 82		
Member States shall provide that where a controller determines the purposes, conditions and means of the processing of personal data jointly with others, the joint controllers must determine the respective responsibilities for compliance with the provisions adopted pursuant to this Directive, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them.	***1.*** Member States shall provide that where a controller determines the purposes~~, conditions~~ and means of the processing of personal data jointly with others, the joint controllers shall determine the respective responsibilities for compliance with the provisions adopted pursuant to this Directive, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of ~~an~~ ***a legally binding*** arrangement between them.	1. Member States shall provide that where two or more controllers jointly determine the purposes and means of the processing of personal data, they are joint controllers. They shall in a transparent manner (...) determine their respective responsibilities for compliance with the provisions adopted pursuant to this Directive, in particular as regards (…) exercising of the rights of the data subject (…) and their respective duties to provide the information referred to in Article 10a, 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. Member States may designate which of the joint controllers can act as single point of contact for data subjects to exercise their rights.	

	2. Unless the data subject has been informed which of the joint controllers is responsible pursuant to paragraph 1, the data subject may exercise his or her rights under this Directive in respect of and against each of any two or more joint controllers.	1a. Without prejudice to Article 17, Member States may provide that the data subject may exercise his or her rights under the provisions adopted pursuant to this Directive in respect of and against each of the controllers.	

Article 21	***Article 21***	***Article 21***	
Processor	***Processor***	***Processor***	
	Amendment 83		
1. Member States shall provide that where a processing operation is carried out on behalf of a controller, the controller must choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of the provisions adopted pursuant to this Directive and ensure the protection of the rights of the data subject.	1. Member States shall provide that where a processing is carried out on behalf of a controller, the controller ~~must~~***shall*** choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of the provisions adopted pursuant to this Directive and ensure the protection of the rights of the data subject***, in particular in respect of the technical security measures and organisational measures governing the processing to be carried out and to ensure compliance with those measures***.	1. Member States shall provide that the controller shall use only (…) processors providing sufficient guarantees to implement appropriate technical and organisational measures (…) in such a way that the processing will meet the requirements of the provisions adopted pursuant to this Directive (…).	

		1a. Member States shall provide that the processor shall not enlist another processor without the prior specific or general written consent of the controller. In the latter case, the processor should always inform the controller on any intended changes concerning the addition or replacement of other processors, thereby giving the opportunity to the controller to object to such changes.	
2. Member States shall provide that the carrying out of processing by a processor must be governed by a legal act binding the processor to the controller and stipulating in particular that the processor shall act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited.	2. Member States shall provide that the carrying out of processing by ***means of*** a processor must be governed by a ***contract or*** legal act binding the processor to the controller and stipulating in particular that the processor shall ~~act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited.~~***:***	2. Member States shall provide that the carrying out of processing by a processor shall be governed by a legal act under Union or Member State law, including a contract, binding the processor to the controller, setting 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, the rights of the controller and stipulating in particular that the processor shall act only on instructions from the controller (…).	

	(a) act only on instructions from the controller;		
	(b) employ only staff who have agreed to be bound by an obligation of confidentiality or are under a statutory obligation of confidentiality;		
	(c) take all required measures pursuant to Article 27;		
	(d) engage another processor only with the permission of the controller and therefore inform the controller of the intention to engage another processor in such a timely fashion that the controller has the possibility to object;		
	(e) insofar as it is possible given the nature of the processing, adopt in agreement with controller the necessary technical and organisational requirements 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) assist the controller in ensuring compliance with the obligations pursuant to Articles 25a to 29;		
	(g) return all results to the controller after the end of the processing and not otherwise process the personal data and delete existing copies unless Union or Member State law requires its storage;		
	(h) make available to the controller and the supervisory authority all the information necessary to verify compliance with the obligations laid down in this Article;		
	(i) take into account the principle of data protection by design and default.		
	2a. The controller and the processor shall document in writing the controller's instructions and the processor's obligation referred to in paragraph 2.		

3. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 20.	3. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 20.	3. deleted	
Article 22	***Article 22***	***Article 22***	
Processing under the authority of the controller and processor	***Processing under the authority of the controller and processor***	***Processing under the authority of the controller and processor***	
	Amendment 84		
Member States shall provide that the processor and any person acting under the authority of the controller or of the processor, who has access to personal data, may only process them on instructions from the controller or where required by Union or Member State law.	***1.*** Member States shall provide that the processor and any person acting under the authority of the controller or of the processor, who has access to personal data, may only process them on instructions from the controller or where required by Union or Member State law.	deleted	
	1a. Where the processor is or becomes the determining party in relation to the purposes, means, or methods of data processing or does not act exclusively on the instructions of the controller, it shall be considered a joint controller pursuant to Article 20.		

Article 23	***Article 23***	***Article 23***	
Documentation	***Documentation***	***Records of categories of personal data processing activities***	
	Amendment 85		
1. Member States shall provide that each controller and processor maintains documentation of all processing systems and procedures under their responsibility.	1. Member States shall provide that each controller and processor maintains documentation of all processing systems and procedures under their responsibility.	1. Member States shall provide that each controller (...) shall maintain a record of all categories of personal data processing activities (…) under its responsibility. This record shall contain (…) the following information:	
		(a) *the name and contact details of the controller and any joint controller* (…) and data protection officer, if any; (b) *the purposes of the processing*; (c) *the (...) categories of recipients* to whom the personal data have been or will be disclosed, in particular recipients in third countries;	Moved from Article 23(2)

		(d) a description of the categories of personal data concerning data subjects; (e) where applicable, the categories of transfers of personal data to a third country or an international organisation; (f) where possible, the envisaged time limits for erasure of the different categories of data; (g) where possible, a general description of the technical and organisational security measures referred to in Article 27(1).	
2. The documentation shall contain at least the following information:	2. The documentation shall contain at least the following information:	2. deleted.	Text moved to Article 23(1)
(a) the name and contact details of the controller, or any joint controller or processor;	(a) the name and contact details of the controller, or any joint controller or processor;		Article 23(1) (a)
	(aa) a legally binding agreement, where there are joint controllers; a list of processors and activities carried out by processors;		

(b) the purposes of the processing;	(b) the purposes of the processing;		Article 23(1) (b)
	(ba) an indication of the parts of the controller's or processor's organisation entrusted with the processing of personal data for a particular purpose;		
	(bb) a description of the category or categories of data subjects and of the data or categories of data relating to them;		
(c) the recipients or categories of recipients of the personal data;	(c) the recipients or categories of recipients of the personal data;		Article 23(1) (c)
	(ca) where applicable, information about the existence of profiling, of measures based on profiling, and of mechanisms to object to profiling;		
	(cb) intelligible information about the logic involved in any automated processing;		

(d) transfers of data to a third country or an international organisation, including the identification of that third country or international organisation.	(d) transfers of data to a third country or an international organisation, including the identification of that third country or international organisation ~~.~~ ***and the legal grounds on which the data are transferred; a substantive explanation shall be given when a transfer is based on Articles 35 or 36 of this Directive;***		Article 23(1) (e)
	(da) the time limits for erasure of the different categories of data;		Article 23(1) (f)
	(db) the results of the verifications of the measures referred to in Article 18(1);		
	(dc) an indication of the legal basis of the processing operation for which the data are intended.		
		2a. Member States shall provide that each processor shall maintain a record of all categories of personal data 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; (b) the name and contact details of the data protection officer, if any; (c) the categories of processing carried out on behalf of each controller;	
		(d) where possible, a general description of the technical and organisational security measures referred to in Article 27(1).	
		2b. The records referred to in paragraphs 1 and 2a shall be in writing, including in an electronic or other non-legible form which is capable of being converted into a legible form.	
3. The controller and the processor shall make the documentation available, on request, to the supervisory authority.	3. The controller and the processor shall make ~~the~~***all*** documentation available, on request, to the supervisory authority.	3. On request, the controller and the processor shall make the record available to the supervisory authority.	

Article 24	***Article 24***	***Article 24***	
Keeping of records	***Keeping of records***	***<u>Logging</u>***	
	Amendment 86		
1. Member States shall ensure that records are kept of at least the following processing operations: collection, alteration, consultation, disclosure, combination or erasure. The records of consultation and disclosure shall show in particular the purpose, date and time of such operations and as far as possible the identification of the person who consulted or disclosed personal data.	1. Member States shall ensure that records are kept of at least the following processing operations: collection, alteration, consultation, disclosure, combination or erasure. The records of consultation and disclosure shall show in particular the purpose, date and time of such operations and as far as possible the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such data.	1. <u>Unless it proves to be impossible or involves disproportionate effort,</u> Member States shall ensure that <u>logs</u> are kept of at least the following processing operations <u>in automated processing systems</u>: collection, alteration, consultation, disclosure, combination or erasure. The <u>logs</u> of consultation and disclosure shall show (…) the <u>reason</u>, <u>the</u> date and <u>the</u> time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data.	

2. The records shall be used solely for the purposes of verification of the lawfulness of the data processing, self-monitoring and for ensuring data integrity and data security.	2. The records shall be used solely for the purposes of verification of the lawfulness of the data processing, self-monitoring and for ensuring data integrity and data security***, or for purposes of auditing, either by the data protection officer or by the data protection authority***.	2. The logs shall be used (...) for (...) verification of the lawfulness of the data processing, self-monitoring and for ensuring data integrity and data security.	
	2a. The controller and the processor shall make the records available, on request, to the supervisory authority.		

Article 25	***Article 25***	***Article 25***	
Cooperation with the supervisory authority	***Cooperation with the supervisory authority***	***Cooperation with the supervisory authority***	
	Amendment 87		
1. Member States shall provide that the controller and the processor shall co-operate, on request, with the supervisory authority in the performance of its duties, in particular by providing all information necessary for the supervisory authority to perform its duties.	1. Member States shall provide that the controller and the processor shall co-operate, on request, with the supervisory authority in the performance of its duties, in particular by providing ~~all~~ ***the*** information ~~necessary for the supervisory authority to perform its duties~~***referred to in point (a) of Article 46(2) and by granting access as provided in point (b) of Article 46(2)***.	1. deleted	

2. In response to the supervisory authority's exercise of its powers under points (a)and (b) of Article 46, the controller and the processor shall reply to the supervisory authority within a reasonable period. The reply shall include a description of the measures taken and the results achieved, in response to the remarks of the supervisory authority.	2. In response to the supervisory authority's exercise of its powers under points (a) and (b) of Article 46***(1)***, the controller and the processor shall reply to the supervisory authority within a reasonable period ***to be specified by the supervisory authority***. The reply shall include a description of the measures taken and the results achieved, in response to the remarks of the supervisory authority.	2. deleted	

	Amendment 88		
	Article 25a (new)		
	Data Protection impact assessment		
	1. Member States shall provide that the controller or the processor, acting on the controller's behalf, shall carry out an assessment of the impact of the envisaged processing systems and procedures on the protection of personal data, where the processing operations are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, prior to new processing operations or the earliest as possible in case of existing processing operations.		
	2. In particular the following processing operations are likely to present such specific risks as referred to in paragraph 1:		

	(a) processing of personal data in large scale filing systems for the purposes of the prevention, detection, investigation or prosecution of criminal offences and the execution of criminal penalties;		
	(b) processing of special categories of personal data as referred to in Article 8, of personal data related to children and of biometric and location data for the purposes of the prevention, detection, investigation or prosecution of criminal offences and the execution of criminal penalties;		
	(c) an evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's behaviour, which is based on automated processing and likely to result in measures that produces legal effects concerning the individual or significantly affects the individual;		

	(d) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance); or		
	(e) other processing operations for which the consultation of the supervisory authority is required pursuant to Article 26(1).		
	3. The assessment shall contain at least:		
	(a) a systematic description of the envisaged processing operations,		
	(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 and the measures envisaged to address those risks and minimise the volume of personal data which is processed;		

	(d) security measures and mechanisms to ensure the protection of personal data and to demonstrate the compliance with the provisions adopted pursuant to this Directive, taking into account the rights and legitimate interests of the data subjects and other persons concerned;		
	(e) a general indication of the time limits for erasure of the different categories of data;		
	(f) where applicable, a list of the intended transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in Article 36(2), the documentation of appropriate safeguards.		
	4. If the controller or the processor has designated a data protection officer, he or she shall be involved in the impact assessment proceeding.		

	5. Member States shall provide that the controller consults the public on the intended processing, without prejudice to the protection of the public interest or the security of the processing operations.		
	6. Without prejudice to the protection of the public interest or the security of the processing operations, the assessment shall be made easily accessible to the public.		
	7. The Commission shall be empowered to adopt, after requesting an opinion of the European Data Protection Board, delegated acts in accordance with Article 56 for the purpose of specifying further the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability.		

Article 26	***Article 26***	***Article 26***	
Prior consultation of the supervisory authority	***Prior consultation of the supervisory authority***	***Prior consultation of the supervisory authority***	
	Amendment 89		
1. Member States shall ensure that the controller or the processor consults the supervisory authority prior to the processing of personal data which will form part of a new filing system to be created where:	1. Member States shall ensure that the controller or the processor consults the supervisory authority prior to the processing of personal data ~~which will form part of a new filing system to be created~~***in order to ensure the compliance of the intended processing with the***	1. Member States shall ensure that the controller or the processor consults the supervisory authority prior to the processing of personal data which will form part of a new filing system to be created where:	
	provisions adopted pursuant to this Directive and in particular to mitigate the risks involved for the data subjects where:		
(a) special categories of data referred to in Article 8 are to be processed;	(a) ~~special categories of data referred to in Article 8 are to be processed~~***a data protection impact assessment as provided for in Article 25a indicates that processing operations by virtue of their nature, their scope and/or their purposes, are likely to present a high degree of specific risks***; ***or***	(a) special categories of <u>personal</u> data referred to in Article 8 are to be processed;	

(b) the type of processing, in particular using new technologies, mechanisms or procedures, holds otherwise specific risks for the fundamental rights and freedoms, and in particular the protection of personal data, of data subjects.	(b) ~~the type of processing, in particular using new technologies, mechanisms or procedures, holds otherwise specific risks for the fundamental rights and freedoms, and in particular the protection of personal data, of data subjects~~ ***the supervisory authority deems it necessary to carry out a prior consultation on specified processing operations which are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes***.	(b) the type of processing, in particular <u>where</u> using new technologies, mechanisms or procedures, <u>involves</u> <u>high</u> risk for the (…) rights and freedoms (…) of data subjects.	
	1a. Where the supervisory authority determines in accordance with its power that the intended processing does not comply with the provisions adopted pursuant to this Directive, in particular where risks are insufficiently identified or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy such non-compliance.		

		1a. Member States shall ensure that the supervisory authority is consulted during the preparation of proposals for legislative or regulatory measures which provide for the processing of personal data referred to in paragraph (1).	
2. Member States may provide that the supervisory authority establishes a list of the processing operations which are subject to prior consultation pursuant to paragraph 1.	2. Member States ~~may~~***shall*** provide that the supervisory authority ~~establishes,~~ ***after consulting the European Data Protection Board, shall establish*** a list of the processing operations which are subject to prior consultation pursuant to ***point (b) of*** paragraph 1.	2. Member States may provide that the supervisory authority establishes a list of the processing operations which are subject to prior consultation pursuant to paragraph 1.	
	2a. Member States shall provide that the controller or processor shall provide the supervisory authority with the data protection impact assessment pursuant to Article 25a and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.		

	2b. If the supervisory authority is of the opinion that the intended processing does not comply with the provisions adopted pursuant to this Directive or that the risks are insufficiently identified or mitigated, it shall make appropriate proposals to remedy such non-compliance.	3. Member States shall provide that where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 does not comply with the provisions adopted pursuant to this Directive, in particular where risks are insufficiently identified or mitigated, the supervisory authority shall within a maximum period of 6 weeks following the request for consultation give advice to the data controller, in writing. This period may be extended for a further month, taking into account the complexity of the intended processing. Where the extended period applies, the controller or processor shall be informed within one month of receipt of the request of the reasons for the delay.	

	2c. Member States may consult the supervisory authority in the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing under this Directive, and in particular to mitigate the risks involved for the data subjects.		

SECTION 2 DATA SECURITY	SECTION 2 DATA SECURITY	SECTION 2 DATA SECURITY	
Article 27	***Article 27***	***Article 27***	
Security of processing	***Security of processing***	***Security of processing***	
	Amendment 90		
1. Member States shall provide that the controller and the processor implements appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected, having regard to the state of the art and the cost of their implementation.	1. Member States shall provide that the controller and the processor ***implements*** appropriate technical and organisational measures ***and procedures*** to ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected, having regard to the state of the art and the cost of their implementation.	1. Having regard to available technology and the costs of implementation and taking into account the nature, scope, context and purposes of the processing as well as the likelihood and severity of the risk for the rights and freedoms of individuals, Member States shall provide that the controller and the processor implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (…).	

2. In respect of automated data processing, each Member State shall provide that the controller or processor, following an evaluation of the risks, implements measures designed to:	2. In respect of automated data processing, each Member State shall provide that the controller or processor, following an evaluation of the risks, implements measures designed to:	2. In respect of automated data processing, each Member State shall provide that the controller or processor, following an evaluation of the risks, implements measures designed to:	
(a) deny unauthorised persons access to data-processing equipment used for processing personal data (equipment access control);	(a) deny unauthorised persons access to data-processing equipment used for processing personal data (equipment access control);	(a) deny unauthorised persons access to data-processing equipment used for processing personal data (equipment access control);	
(b) prevent the unauthorised reading, copying, modification or removal of data media (data media control);	(b) prevent the unauthorised reading, copying, modification or removal of data media (data media 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);	(c) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data (storage 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 data-processing systems by unauthorised persons using data communication equipment (user control);	(d) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment (user control);	(d) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment (user control);	

(e) ensure that persons authorised to use an automated data-processing system only have access to the data covered by their access authorisation (data access control);	(e) ensure that persons authorised to use an automated data-processing system only have access to the data covered by their access authorisation (data access control);	(e) ensure that persons authorised to use an automated data-processing system only have access to the data covered by their access authorisation (data access control);	
(f) ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data communication equipment (communication control);	(f) ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data communication equipment (communication control);	(f) ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data communication equipment (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);	(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);	(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 the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media (transport control);	(h) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media (transport control);	(h) prevent the 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 case of interruption, be restored (recovery);	(i) ensure that installed systems may, in case of interruption, be restored (recovery);	(i) ensure that installed systems may, in case of interruption, be restored (recovery);	

(j) ensure that the functions of the 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).	(j) ensure that the functions of the 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).	(j) ensure that the functions of the 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).	
	(ja) ensure that in case of sensitive personal data processing according to Article 8, additional security measures have to be in place, in order to guarantee situation awareness of risks and the ability to take preventive, corrective and mitigating action in near real time against vulnerabilities or incidents detected that could pose a risk to the data.		
	2a. Member States shall provide that processors may be appointed only if they guarantee that they observe the requisite technical and organisational measures under paragraph 1 and comply with the instructions under point (a) of Article 21(2). The competent authority shall monitor the processor in those respects.		

3. The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, notably encryption standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 57(2).	3. The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, notably encryption standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 57(2).	3. deleted	

Article 28	*Article 28*	*Article 28*	
Notification of a personal data breach to the supervisory authority	***Notification of a personal data breach to the supervisory authority***	***Notification of a personal data breach to the supervisory authority***	
	Amendment 91		
1. Member States shall provide that in the case of a personal data breach, the controller notifies, without undue delay and, where feasible, not later than 24 hours after having become aware of it, the personal data breach to the supervisory authority. The controller shall provide, on request, to the supervisory authority a reasoned justification in cases where the notification is not made within 24 hours.	1. Member States shall provide that in the case of a personal data breach, the controller notifies, without undue delay and, where feasible, not later than 24 hours ~~after having become aware of it~~, the personal data breach to the supervisory authority. The controller shall provide, on request, to the supervisory authority a reasoned justification in cases ~~where the notification is not made within 24 hours~~ ***of any delay***.	1. Member States shall provide that in the case of a personal data breach which is likely to result in a high risk for the rights and freedoms of data subjects**,** the controller notifies, without undue delay and, where feasible, not later than 72 hours after having become aware of it, the personal data breach to the supervisory authority (…). The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 72 hours.	
		1a. The notification referred to in paragraph 1 shall not be required if a communication of the data subject is not required under Article 29(3)(a) and (b).	

2. The processor shall alert and inform the controller immediately after having become aware of a personal data breach.	2. The processor shall alert and inform the controller ~~immediately~~ ***without undue delay*** after ~~having become aware~~ ***the establishment*** of a personal data breach.	2. The processor shall alert and inform the controller without undue delay after having become aware of a personal 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 the categories and number of data subjects concerned and the categories and number of data records concerned;	(a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned;	(a) describe the nature of the personal data breach (…);	
(b) communicate the identity and contact details of the data protection officer referred to in Article 30 or other contact point where more information can be obtained;	(b) communicate the identity and contact details of the data protection officer referred to in Article 30 or other contact point where more information can be obtained;	(b) communicate the identity and contact details of the data protection officer (…) or other contact point where more information can be obtained;	
(c) recommend measures to mitigate the possible adverse effects of the personal data breach;	(c) recommend measures to mitigate the possible adverse effects of the personal data breach;	(c) deleted	
(d) describe the possible consequences of the personal data breach;	(d) describe the possible consequences of the personal data breach;	(d) describe the likely consequences of the personal data breach identified by the controller,	

(e) describe the measures proposed or taken by the controller to address the personal data breach.	(e) describe the measures proposed or taken by the controller to address the personal data breach ***and mitigate its effects***.	(e) describe the measures <u>taken or proposed to be taken</u> by the controller to address the personal data breach; <u>and</u>	
		<u>(f) where appropriate, indicate measures to mitigate the possible adverse effects of the personal data breach.</u>	
	In case all information cannot be provided without undue delay, the controller can complete the notification in a second phase.	<u>3a. Where, and in so far as, it is not possible to provide the information referred to in paragraph 3 (d), (e) and (f) at the same time as the information referred to in points (a) and (b) of paragraph 3, the controller shall provide this information without undue further delay.</u>	
4. Member States shall provide that the controller documents any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose.	4. Member States shall provide that the controller documents any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must ***be sufficient to*** enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose.	4. Member States shall provide that the controller documents any personal data breaches <u>referred to in paragraph 1</u>, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. (...)	

	4a. The supervisory authority shall keep a public register of the types of breaches notified.		
		4a. Subject to paragraph 1a Member States shall provide that where the data breach involves personal data that have been transmitted by or to the controller of another Member State, the information referred to in paragraph 3 shall be communicated to the controller of this Member State without undue delay.	
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 56 for the purpose of specifying further the criteria and requirements for establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.	5. The Commission shall be empowered to adopt***, after requesting an opinion of the European Data Protection Board,*** delegated acts in accordance with Article 56 for the purpose of specifying further the criteria and requirements for establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor ~~is~~ ***are*** required to notify the personal data breach.	5. deleted	

6. The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 57(2).	6. The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 57(2).	6. deleted	

Article 29	*Article 29*	*Article 29*	
Communication of a personal data breach to the data subject	***Communication of a personal data breach to the data subject***	***Communication of a personal data breach to the data subject***	
	Amendment 92		
1. Member States shall provide that when the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 28, communicate the personal data breach to the data subject without undue delay.	1. Member States shall provide that when the personal data breach is likely to adversely affect the protection of the personal data ~~or~~ ***,*** ***the*** privacy***, the rights or the legitimate interests*** of the data subject, the controller shall, after the notification referred to in Article 28, communicate the personal data breach to the data subject without undue delay.	1. Subject to paragraphs 3 and 4 of this Article, Member States shall provide that when the personal data breach is likely to result in a high risk for the rights and freedoms (…) of the data subject 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 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) and (c) of Article 28(3).	2. The communication to the data subject referred to in paragraph 1 shall ***be comprehensive and use clear and plain language. It shall*** describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b)***,*** ~~and~~ (c) ***and (d)*** of Article 28(3) ***and information about the rights of the data subject, including redress***.	2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and shall contain at least the information referred to in Article 28(3) (b)(e) and (f).	

3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the personal data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.	3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the personal data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.	3. The communication (…) to the data subject referred to in paragraph 1 shall not be required if: (a) the controller (…) has implemented appropriate technological 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 data unintelligible to any person who is not authorised to access it, such as encryption; or (b) the controller has taken subsequent measures which ensure that the high risk for the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; or	

		(c) it would involve disproportionate effort, in particular owing to the number of cases involved. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.	
	3a. Without prejudice to the controller's obligation to notify the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.		
4. The communication to the data subject may be delayed, restricted or omitted on the grounds referred to in Article 11(4).	4. The communication to the data subject may be delayed~~,~~ ***or*** restricted ~~or omitted~~ on the grounds referred to in Article 11(4).	4. The communication to the data subject referred to in paragraph 1 may be delayed, restricted or omitted on the grounds referred to in Article 10a (3).	

SECTION 3 DATA PROTECTION OFFICER	SECTION 3 DATA PROTECTION OFFICER	SECTION 3 DATA PROTECTION OFFICER	
Article 30	***Article 30***	***Article 30***	
Designation of the data protection officer	***Designation of the data protection officer***	***Designation of the data protection officer***	
	Amendment 93		
1. Member States shall provide that the controller or the processor designates a data protection officer.	1. Member States shall provide that the controller or the processor designates a data protection officer.	1. Member States may, or where required by Union law, shall, provide that the controller or the processor designates a data protection officer.	

2. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 32.	2. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 32. ***The necessary level of expert knowledge shall be determined, in particular, according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.***	2. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 32, particularly the absence of any conflict of interests.	
	2a. Member States shall provide that the controller or the processor ensures that any other professional duties of the data protection officer are compatible with that person's tasks and duties as data protection officer and do not result in a conflict of interests.		

	2b. The data protection officer shall be appointed for a period of at least four years. The data protection officer may be reappointed for further terms. During the term of office, the data protection officer may only be dismissed from that function, if he or she no longer fulfils the conditions required for the performance of his or her duties.		
	2c. Member States shall provide the data subject with the right to contact the data protection officer on all issues related to the processing of his or her personal data.		
3. The data protection officer may be designated for several entities, taking account of the organisational structure of the competent authority.	3. The data protection officer may be designated for several entities, taking account of the organisational structure of the competent authority.	3. A single data protection officer may be designated for several competent authorities, taking account of their organisational structure and size.	

	3a. Member States shall provide that the controller or the processor shall communicate the name and contact details of the data protection officer to the supervisory authority and to the public.		
		4. *Member States shall provide that the controller or the processor ensures that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.*	Moved from Article 31(1)
		5. *The controller or processor shall ensure that the data protection officer is provided with the means to perform (...) the tasks referred to under Article 32 effectively and* can act in an *independent* manner with respect to the performance of his or her tasks.	Moved from Article 31(2)

Article 31	*Article 31*	*Article 31*	
Position of the data protection officer	***Position of the data protection officer***	***Position of the data protection officer***	
	Amendment 94		
1. Member States shall provide that the controller or the processor ensures that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.	1. Member States shall provide that the controller or the processor ensures that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.	Moved to Article 30 (4)	
2. The controller or processor shall ensure that the data protection officer is provided with the means to perform duties and tasks referred to under Article 32 effectively and independently, and does not receive any instructions as regards the exercise of the function.	2. The controller or processor shall ensure that the data protection officer is provided with the means to perform duties and tasks referred to under Article 32 effectively and independently, and does not receive any instructions as regards the exercise of the function.	Moved to Article 30 (5)	

	2a. The controller or the processor shall support the data protection officer in performing his or her tasks and shall provide all the means, including staff, premises, equipment, continuous professional training and any other resources necessary to carry out the duties and tasks referred to in Article 32, and to maintain his or her professional knowledge.		
Article 32	***Article 32***	***Article 32***	
Tasks of the data protection officer	***Tasks of the data protection officer***	***Tasks of the data protection officer***	
	Amendment 95		
Member States shall provide that the controller or the processor entrusts the data protection officer at least with the following tasks:	Member States shall provide that the controller or the processor entrusts the data protection officer at least with the following tasks:	Member States shall provide that the controller or the processor entrusts the data protection officer (…) with the following tasks:	

(a) to inform and advise the controller or the processor of their obligations in accordance with the provisions adopted pursuant to this Directive and to document this activity and the responses received;	(a) ***to raise awareness,*** to inform and advise the controller or the processor of their obligations in accordance with the provisions adopted pursuant to this Directive***, in particular with regard to technical and organisational measures and procedures,*** and to document this activity and the responses received;	(a) to inform and advise the controller or the processor of their obligations in accordance with the provisions adopted pursuant to this Directive and other Union or Member State data protection provisions (…);	
(b) to monitor the implementation and application of the policies in relation to the protection of personal data, including the assignment of responsibilities, the training of staff involved in the processing operations and the related audits;	(b) to monitor the implementation and application of the policies in relation to the protection of personal data, including the assignment of responsibilities, the training of staff involved in the processing operations and the related audits;	(b) to monitor compliance with provisions adopted pursuant to this Directive, with other Union or Member State data protection provisions and with (…) the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities**,** awareness-raising and training of staff involved in the processing operations and the related audits;	

(c) to monitor the implementation and application of the provisions adopted pursuant to this Directive, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under the provisions adopted pursuant to this Directive;	(c) to monitor the implementation and application of the provisions adopted pursuant to this Directive, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under the provisions adopted pursuant to this Directive;	(c) deleted	
(d) to ensure that the documentation referred to in Article 23 is maintained;	(d) to ensure that the documentation referred to in Article 23 is maintained;	(d) deleted	
(e) to monitor the documentation, notification and communication of personal data breaches pursuant to Articles 28 and 29;	(e) to monitor the documentation, notification and communication of personal data breaches pursuant to Articles 28 and 29;	(e) deleted	
(f) to monitor the application for prior consultation to the supervisory authority, if required pursuant to Article 26;	(f) to monitor ***the application of the data protection impact assessment by the controller or processor and*** the application for prior consultation to the supervisory authority, if required pursuant to Article 26***(1)***-;	(f) deleted	

(g) to monitor the response to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, co-operating with the supervisory authority at the latter's request or on his own initiative;	(g) to monitor the response to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, co-operating with the supervisory authority at the latter's request or on his own initiative;	(g) to monitor the responses to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, to co-operate with the supervisory authority at the latter's request or on the data protection officer's own initiative;	

(h) to act as the contact point for the supervisory authority on issues related to the processing and consult with the supervisory authority, if appropriate, on the data protection officer's own initiative;	(h) to act as the contact point for the supervisory authority on issues related to the processing and consult with the supervisory authority, if appropriate, on the data protection officer's own initiative.	(h) to act as the contact point for the supervisory authority on issues related to the processing of personal data, including the prior consultation referred to in Article 26, and consult, (…) as appropriate, on any other matter.	

CHAPTER V TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS	CHAPTER V TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS	CHAPTER V TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS	
Article 33	***Article 33***	***Article 33***	
General principles for transfers of personal data	***General principles for transfers of personal data***	***General principles for transfers of personal data***	
	Amendment 96		
Member States shall provide that any transfer of personal data by competent authorities that is undergoing processing or is intended for processing after transfer to a third country, or to an international organisation, including further onward transfer to another third country or international organisation, may take place only if:	Member States shall provide that any transfer of personal data by competent authorities that are undergoing processing or are intended for processing after transfer to a third country, or to an international organisation, including further onward transfer to another third country or international organisation, may take place only if:	1. Member States shall provide that any transfer of personal data by competent authorities (…) to a third country, or to an international organisation, including further onward transfer to another third country or international organisation, may take place only if:	

(a) the transfer is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; and	(a) the ***specific*** transfer is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; and	(a) the transfer is necessary for the purposes set out in Article 1 (1); and,	
	(aa) the data are transferred to a controller in a third country or international organisation that is a public authority competent for the purposes referred to in Article 1(1); and		
	(ab) the conditions laid down in this Chapter are complied with by the controller and the processor, including for onward transfers of personal data from a third country or an international organisation to another third country or to another international organisation; and		
(b) the conditions laid down in this Chapter are complied with by the controller and processor.	(b) the ~~conditions laid down in this Chapter~~ ***other provisions adopted pursuant to this Directive*** are complied with by the controller and processor~~.~~***; and***	***Deleted***	

	(ba) the level of protection of the personal data individuals guaranteed in the Union by this Directive is not undermined; and	(c) the controller in the third country or international organisation is an authority competent for the purposes set out in Article 1(1); and	
	(bb) the Commission has decided under the conditions and procedure referred to in Article 34 that the third country or international organisation in question ensures an adequate level of protection; or	(d) in case personal data are transmitted or made available from another Member State, that Member State has given its prior authorisation to the transfer in compliance with its national law and	
	(bc) appropriate safeguards with respect to the protection of personal data have been adduced in a legally binding instrument as referred to in Article 35.	(e) the Commission has decided pursuant to Article 34 that the third country or international organisation in question ensures an adequate level of protection or in the absence of an adequacy decision poursuant to Article 34, where appropriate safeguards are adduced or exist pursuant to Article 35.	

	Member States shall provide that further onward transfers referred to in paragraph 1 of this Article may only take place if, in addition to the conditions laid down in that paragraph:	2. Member States shall provide that transfers without the prior authorisation by another Member State in accordance with point (d) shall be permitted only if the transfer of the personal data is necessary for the prevention of an immediate and serious threat to public security of a Member State or a third country or to essential interests of a Member State and the prior authorisation cannot be obtained in good time. The authority responsible for giving prior authorisation shall be informed without delay.	
		3. Member States shall provide that in the absence of an adequacy decision pursuant to Article 34 or of appropriate safeguards in accordance with Article 35, a transfer may only take place where derogations for specific situations apply pursuant to Article 36 and the conditions laid down in points (a), (c) and (d) of paragraph 1 and, as the case may be, (…) in paragraph 2 of this Article are complied with.	

	(a) the onward transfer is necessary for the same specific purpose as the original transfer; and		
	(b) the competent authority that carried out the original transfer authorises the onward transfer.		

Article 34	***Article 34***	***Article 34***	
Transfers with an adequacy decision	***Transfers with an adequacy decision***	***Transfers with an adequacy decision***	
	Amendment 97		
1. Member States shall provide that a transfer of personal data to a third country or an international organisation may take place where the Commission has decided in accordance with Article 41 of Regulation (EU) …./2012 or in accordance with paragraph 3 of this Article 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. Such transfer shall not require any further authorisation.	1. Member States shall provide that a transfer of personal data to a third country or an international organisation may take place where the Commission has decided ~~in accordance with Article 41 of Regulation (EU) …./2012 or~~ in accordance with paragraph 3 of this Article 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. Such transfer shall not require any ~~further~~ ***specific*** authorisation.	1. Member States shall provide that a transfer of personal data to a third country or a territory or one or more specified sectors within a third country or an international organisation may take place where the Commission has decided in accordance with Article 41 of Regulation EU/XXX or in accordance with paragraph 3 of this Article that the third country or a territory or specified sector within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any specific authorisation.	

2. Where no decision adopted in accordance with Article 41 of Regulation (EU) …./2012 exists, the Commission shall assess the adequacy of the level of protection, giving consideration to the following elements:	2. ~~Where no decision adopted in accordance with Article 41 of Regulation (EU) …./2012 exists~~***When assessing the adequacy of the level of protection***, the Commission shall ~~assess the adequacy of the level of protection, giving~~ ***give*** consideration to the following elements:	2. Where no decision adopted in accordance with Article 41 of Regulation EU/XXX (…) applies, the Commission shall assess the adequacy of the level of protection, in particular taking into account the following elements:	
(a) the rule of law, relevant legislation in force, both general and sectoral, including concerning public security, defence, national security and criminal law as well as the security measures which are complied with in that country or by that international organisation; as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred;	(a) the rule of law, relevant legislation in force~~, both general and sectoral,~~ including concerning public security, defence, national security and criminal law as well as the ***implementation of this legislation and the*** security measures which are complied with in that country or by that international organisation; ***jurisprudential precedents*** as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred;	(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, data protection rules (…)including concerning public security, defence, national security and criminal law as well as (…) security measures, including rules for onward transfer of personal data to another third country or international organisation, which are complied with in that country or by that international organisation; as well as the existence of effective and enforceable data subject rights and effective administrative and judicial redress for data subjects (…) whose personal data are being transferred;	

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or international organisation in question responsible for ensuring compliance with the data protection rules, for assisting and advising the data subject in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States; and	(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or international organisation in question responsible for ensuring compliance with the data protection rules, ***including sufficient sanctioning powers,*** for assisting and advising the data subject in exercising his or her rights and for co-operation with the supervisory authorities of the Union and of Member States; and	(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility (…) for ensuring and enforcing compliance with the data protection rules including adequate sanctioning powers for assisting and advising (…) data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States; and	
(c) the international commitments the third country or international organisation in question has entered into.	(c) the international commitments the third country or international organisation in question has entered into***, in particular any legally binding conventions or instruments with respect to the protection of personal data***.	(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.	

		2a. The European Data Protection Board shall give the Commission an opinion for the assessment of the adequacy of the level of protection in a third country or international organization, including for the assessment whether a third country or the territory or the international organization or the specified sector no longer ensures an adequate level of protection.	
3. The Commission may decide, within the scope of this Directive, that a third country or a territory or a processing sector within that third country or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 57(2).	3. The Commission ~~may~~ ***shall be empowered to adopt, after requesting an opinion of the European Data Protection Board, delegated acts in accordance with Article 56 to*** decide, within the scope of this Directive, that a third country or a territory or a processing sector within that third country or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. ~~Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 57(2).~~	3. The Commission after assessing the adequacy of the level of protection, may decide, within the scope of this Directive that a third country or a territory or one or more specified sectors within that third country or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority(ies) mentioned in point (b) of paragraph 2. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 57(2).	

4. The implementing act shall specify its geographical and sectoral application, and, where applicable, identify the supervisory authority mentioned in point (b) of paragraph 2.	4. The ~~implementing~~***delegated*** act shall specify its geographical and sectoral application, and~~, where applicable,~~ identify the supervisory authority mentioned in point (b) of paragraph 2.	Deleted	
	4a. The Commission shall, on an on-going basis, monitor developments that could affect the fulfilment of the elements listed in paragraph 2 in third countries and international organisations in relation to which a delegated act pursuant to paragraph 3 has been adopted.	4a. The Commission shall monitor the functioning of decisions adopted pursuant to paragraph 3.	

5. The Commission may decide within the scope of this Directive that a third country or a territory or a processing sector within that third country or an international organisation does not ensure an adequate level of protection within the meaning of paragraph 2, in particular in cases where the relevant legislation, both general and sectoral, in force in the third country or international organisation, does not guarantee effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects whose personal data are being transferred. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 57(2), or, in cases of extreme urgency for individuals with respect to their right to personal data protection, in accordance with the procedure referred to in Article 57(3).	5. The Commission ~~may~~***shall be empowered to adopt delegated acts in accordance with Article 56 to*** decide within the scope of this Directive that a third country or a territory or a processing sector within that third country or an international organisation does not ensure an adequate level of protection within the meaning of paragraph 2, in particular in cases where the relevant legislation~~, both general and sectoral,~~ in force in the third country or international organisation, does not guarantee effective and enforceable rights, including effective administrative and judicial redress for data subjects, in particular for those data subjects whose personal data are being transferred. ~~Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 57(2), or, in cases of extreme urgency for individuals with respect to their right to personal data protection, in accordance with the procedure referred to in Article 57(3).~~	5. The Commission may decide within the scope of this Directive that a third country or a territory or a specified sector within that third country or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2, and may, where necessary, repeal, amend or suspend such decision without retro-active effect. The (…) implementing acts shall be adopted in accordance with the examination procedure referred to in Article 57(2), or, in cases of extreme urgency, in accordance with the procedure referred to in Article 57(3).	

		5a. (…) The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.	Moved from Article 34(6)
6. Member States shall ensure that where the Commission decides pursuant to paragraph 5, that any transfer of personal data to the third country or a territory or a processing sector within that third country, or the international organisation in question shall be prohibited, this decision shall be without prejudice to transfers under Article 35(1) or in accordance with Article 36. At the appropriate time, the Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation resulting from the Decision made pursuant to paragraph 5 of this Article.	6. Member States shall ensure that where the Commission decides pursuant to paragraph 5, ~~that~~ any transfer of personal data to the third country or a territory or a processing sector within that third country, or the international organisation in question shall be prohibited~~, this decision shall be without prejudice to transfers under Article 35(1) or in accordance with Article 36~~. At the appropriate time, the Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation resulting from the Decision made pursuant to paragraph 5 of this Article.	6. Member States shall ensure that where a decision pursuant to paragraph 5 is taken, such decision (…) shall be without prejudice to transfers of personal data to the third country, or the territory or the specified sector within that third country, or the international organisation in question pursuant to Articles 35 and 36 (…).	

7. The Commission shall publish in the *Official Journal of the European Union* a list of those third countries, territories and processing sectors within a third country or an international organisation where it has decided that an adequate level of protection is or is not ensured.	7. The Commission shall publish in the *Official Journal of the European Union* a list of those third countries, territories and processing sectors within a third country or an international organisation where it has decided that an adequate level of protection is or is not ensured.	7. The Commission shall publish in the *Official Journal of the European Union* a list of those third countries, territories and specified sectors within a third country and international organisations in respect of which decisions have been taken pursuant to paragraphs 3 (…) and 5.	
8. The Commission shall monitor the application of the implementing acts referred to in paragraphs 3 and 5.	8. The Commission shall monitor the application of the ~~implementing~~ ***delegated*** acts referred to in paragraphs 3 and 5.	***deleted***	

Article 35	***Article 35***	***Article 35***	
Transfers by way of appropriate safeguards	***Transfers by way of appropriate safeguards***	***Transfers by way of appropriate safeguards***	
	Amendment 98		
1. Where the Commission has taken no decision pursuant to Article 34, Member States shall provide that a transfer of personal data to a recipient in a third country or an international organisation may take place where:	1. Where the Commission has taken no decision pursuant to Article 34, ~~Member States shall provide that a~~ ***or decides that a third country, or a territory within that third country, or an international organisation does not ensure an adequate level of protection in accordance with Article 34(5), a controller or processor may not*** transfer ~~of~~ personal data to ~~a recipient in~~ a third country***, or a territory within that third country,*** or an international organisation ~~may take place where:~~***unless the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument.***	(…) In the absence of a decision pursuant to paragraph 3 of Article 34, Member States shall provide that (…) a transfer of personal data to a third country or an international organisation may take place where:	

(a) appropriate safeguards with respect to the protection of personal data have been adduced in a legally binding instrument; or	***deleted***	(a) appropriate safeguards with respect to the protection of personal data have been adduced in a legally binding (…) instrument; or	
(b) the controller or processor has assessed all the circumstances surrounding the transfer of personal data and concludes that appropriate safeguards exist with respect to the protection of personal data.	***deleted***	(b) the controller (…) has assessed all the circumstances surrounding the transfer of personal data and concludes that appropriate safeguards exist with respect to the protection of personal data. Such an assessment may take into account the existing cooperation agreements between Europol and/or Eurojust and third countries which allow for the exchange of personal data.	
2. The decision for transfers under paragraph 1 (b) must be made by duly authorised staff. These transfers must be documented and the documentation must be made available to the supervisory authority on request.	2.~~The decision for transfers under paragraph 1 (b) must be made by duly authorised staff.~~ Those transfers must be ~~documented and the documentation must be made available to the supervisory authority on request~~***authorised by the supervisory authority prior to the transfer***.	***deleted***	

Article 36	*Article 36*	*Article 36*	
Derogations	***Derogations***	***Derogations for (…) specific situations***	
	Amendment 99		
By way of derogation from Articles 34 and 35, Member States shall provide that a transfer of personal data to a third country or an international organisation may take place only on condition that:	***1. Where the Commission decides pursuant to Article 34(5) that an adequate level of protection does not exist, personal data may not be transferred to the third country or to the international organisation in question if, in the case in question, the legitimate interests of the data subject in preventing any such transfer outweigh the public interest in transferring such data.***	1. (…) In the absence of an adequacy decision pursuant to Article 34 or appropriate safeguards pursuant to Article 35, Member States shall provide that, a transfer or a category of transfers of personal data to a third country or an international organisation may take place only on condition that:	
	2. By way of derogation from Articles 34 and 35, Member States shall provide that a transfer of personal data to a third country or an international organisation may take place only on condition that:		
(a) the transfer is necessary in order to protect the vital interests of the data subject or another person; or	(a) the transfer is necessary in order to protect the vital interests of the data subject or another person; or	(a) the transfer is necessary in order to protect the vital interests of the data subject or another person; or	

(b) the transfer is necessary to safeguard legitimate interests of the data subject where the law of the Member State transferring the personal data so provides; or	(b) the transfer is necessary to safeguard legitimate interests of the data subject where the law of the Member State transferring the personal data so provides; or	(b) the transfer is necessary to safeguard legitimate interests of the data subject (…) where the law of the Member State transferring the personal data so provides; or	
(c) the transfer of the data is essential for the prevention of an immediate and serious threat to public security of a Member State or a third country; or	(c) the transfer of the data is essential for the prevention of an immediate and serious threat to public security of a Member State or a third country; or	(c) the transfer of the data is necessary for the prevention of an immediate and serious threat to public security of a Member State or a third country; or	
(d) the transfer is necessary in individual cases for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; or	(d) the transfer is necessary in individual cases for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; or	(d) the transfer is necessary in individual cases for the purposes set out in Article 1 (1); or	
(e) the transfer is 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 penalty.	(e) the transfer is 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 penalty.	(e) the transfer is necessary in an individual cases for the establishment, exercise or defence of legal claims relating to the purposes set out in Article 1 (1).	

		2. Personal data shall not be transferred if the transferring competent authority determines that fundamental rights and freedoms of the data subject concerned override the public interest in the transfer set out in points (d) and (e) of paragraph 1.	
	2a. Processing based on paragraph 2 must have a legal basis in Union law, or the law of the Member State to which the controller is subject; that law must meet public interest objective or the need to protect the rights and freedoms of others, respects the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued.		
	2b. All transfers of personal data decided on the basis of derogations shall be duly justified and shall be limited to what is strictly necessary, and frequent massive transfers of data shall not be allowed.		

	2c. The decision for transfers under paragraph 2 must be made by duly authorised staff. Those transfers must be documented and the documentation must be made available to the supervisory authority on request, including the date and time of the transfer, information about the recipient authority, the justification for the transfer and the data transferred.		
Article 36aa	***Article 36aa***	***Article 36aa***	
		Transfer of personal data to recipients established in third countries	
		1. By way of derogation from Article 33 (1) (c) and without prejudice to any international agreement referred to in paragraph 2, Union or Member States law may provide that the competent authorities may, in individual and specific cases, transfer personal data directly to recipients established in third countries only if the other provisions of this Directive are complied with and the following conditions are fulfilled:	

		(a) the transfer is strictly necessary for the performance of a task of the competent authority as provided for by Union or Member State law for the purposes set out in Article 1(1); and	
		(b) the transferring competent authority determines that no fundamental rights and freedoms of the data subject concerned override the public interest necessitating the transfer in the case at hand.	
		2. An international agreement referred to in paragraph 1 shall be any bilateral or multilateral international agreement in force between Member States and third countries in the field of judicial co-operation in criminal matters and police co-operation.	

Article 37	*Article 37*	*Article 37*	
Specific conditions for the transfer of personal data	***Specific conditions for the transfer of personal data***	***Specific conditions for the transfer of personal data***	
	Amendment 100		
Member States shall provide that the controller informs the recipient of the personal data of any processing restrictions and takes all reasonable steps to ensure that these restrictions are met.	Member States shall provide that the controller informs the recipient of the personal data of any processing restrictions and takes all reasonable steps to ensure that these restrictions are met. ***The controller shall also notify the recipient of the personal data of any update, rectification or erasure of data, and the recipient shall in turn make the corresponding notification in the event that the data have subsequently been transferred.***	deleted	

Article 38	*Article 38*	*Article 38*	
International co-operation for the protection of personal data	***International co-operation for the protection of personal data***	***International co-operation for the protection of personal data***	
	Amendment 101		
1. In relation to third countries and international organisations, the Commission and Member States shall take appropriate steps to:	1. In relation to third countries and international organisations, the Commission and Member States shall take appropriate steps to:	***deleted***	
(a) develop effective international co-operation mechanisms to facilitate the enforcement of legislation for the protection of personal data;	(a) develop effective international co-operation mechanisms to ~~facilitate~~***ensure*** the enforcement of legislation for the protection of personal data;	***deleted***	
(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;	***deleted***	

(c) engage relevant stakeholders in discussion and activities aimed at furthering international co-operation in the enforcement of legislation for the protection of personal data;	(c) engage relevant stakeholders in discussion and activities aimed at furthering international co-operation in the enforcement of legislation for the protection of personal data;	***deleted***	
(d) promote the exchange and documentation of personal data protection legislation and practice.	(d) promote the exchange and documentation of personal data protection legislation and practice~~.~~***;***	***deleted***	

	Amendment 102		
	(da) clarify and consult on jurisdictional conflicts with third countries.		
2. For the purposes of paragraph 1, the Commission shall take appropriate steps to advance the relationship with third countries or with international organisations, and in particular their supervisory authorities, where the Commission has decided that they ensure an adequate level of protection within the meaning of Article 34(3).	2. For the purposes of paragraph 1, the Commission shall take appropriate steps to advance the relationship with third countries or with international organisations, and in particular their supervisory authorities, where the Commission has decided that they ensure an adequate level of protection within the meaning of Article 34(3).	***deleted***	

	Amendment 103		
	Article 38a		
	Report by the Commission		
	The Commission shall submit a report on the application of Articles 33 to 38 to the European Parliament and to the Council at regular intervals. The first report shall be submitted not later than four years after the entry into force of this Directive. For that purpose, the Commission may request information from the Member States and supervisory authorities, which shall supply that information without undue delay. The report shall be made public.		

CHAPTER VI INDEPENDENT SUPERVISORY AUTHORITIES	CHAPTER VI INDEPENDENT SUPERVISORY AUTHORITIES	CHAPTER VI INDEPENDENT SUPERVISORY AUTHORITIES	
SECTION 1 **INDEPENDENT STATUS**	**SECTION 1** **INDEPENDENT STATUS**	**SECTION 1** **INDEPENDENT STATUS**	
Article 39	***Article 39***	***Article 39***	
Supervisory authority	***Supervisory authority***	***Supervisory authority***	
1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application of the provisions adopted pursuant to this Directive and for contributing to its consistent application throughout the Union, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the Union. For this purpose, the supervisory authorities shall co-operate with each other and the Commission.	1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application of the provisions adopted pursuant to this Directive and for contributing to its consistent application throughout the Union, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the Union. For this purpose, the supervisory authorities shall co-operate with each other and the Commission.	1. Each Member State shall provide that one or more <u>independent</u> public authorities are responsible for monitoring the application of the provisions adopted pursuant to this Directive (…).	

		1a. Each supervisory authority shall contribute to the consistent application of this Directive throughout the Union. For this purpose, the supervisory authorities shall co-operate with each other and the Commission in accordance with Chapter VII.	Moved from Article 39(1)
2. Member States may provide that the supervisory authority established in Member States pursuant to Regulation (EU)…./2012 assumes responsibility for the tasks of the supervisory authority to be established pursuant to paragraph 1 of this Article.	2. Member States may provide that the supervisory authority established in Member States pursuant to Regulation (EU)…./2012 assumes responsibility for the tasks of the supervisory authority to be established pursuant to paragraph 1 of this Article.	2. Member States may provide that a supervisory authority established (…) under Regulation EU/XXX may be the supervisory authority referred to in this Directive and assumes responsibility for the tasks of the supervisory authority to be established under paragraph 1 of this Article.	
3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the European Data Protection Board.	3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the European Data Protection Board.	3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which (…) shall represent those authorities in the European Data Protection Board.	

Article 40	***Article 40***	***Article 40***	
Independence	***Independence***	***Independence***	
	Amendment 104		
1. Member States shall ensure that the supervisory authority acts with complete independence in exercising the duties and powers entrusted to it.	1. Member States shall ensure that the supervisory authority acts with complete independence in exercising the duties and powers entrusted to it***, notwithstanding co-operation arrangements pursuant to Chapter VII of this Directive***.	1. Member States shall ensure that each supervisory authority acts with complete independence in performing the tasks and exercising the (…) powers entrusted to it.	
	Amendment 105		
2. Each Member State shall provide that the members of the supervisory authority, in the performance of their duties, neither seek nor take instructions from anybody.	2. Each Member State shall provide that the members of the supervisory authority, in the performance of their duties, neither seek nor take instructions from anybody***, and maintain complete independence and impartiality***.	2. (…) Member States shall provide that the member or (…) members of each supervisory authority, in the performance of their tasks and exercise of their powers in accordance with this Directive, remain free from external influence, whether direct or indirect and neither seek nor take instructions from anybody.	

3. Members of the supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.	3. Members of the supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.	3. deleted	
4. Members of the supervisory authority shall behave, after their term of office, with integrity and discretion as regards the acceptance of appointments and benefits.	4. Members of the supervisory authority shall behave, after their term of office, with integrity and discretion as regards the acceptance of appointments and benefits.	4. deleted	
5. Each Member State shall ensure that the supervisory authority is provided with the adequate human, technical and financial resources, premises and infrastructure necessary for the effective performance of its duties and powers including those to be carried out in the context of mutual assistance, co-operation and active participation in the European Data Protection Board.	5. Each Member State shall ensure that the supervisory authority is provided with the adequate human, technical and financial resources, premises and infrastructure necessary for the effective performance of its duties and powers including those to be carried out in the context of mutual assistance, co-operation and active participation in the European Data Protection Board.	5. (…) Member State<u>s</u> shall ensure that <u>each</u> supervisory authority is provided with the (…) human, technical and financial resources, premises and infrastructure necessary for the effective performance of its <u>tasks</u> and <u>exercise of its</u> powers including those to be carried out in the context of mutual assistance, co-operation and active participation in the European Data Protection Board.	

6. Each Member State shall ensure that the supervisory authority must have its own staff which shall be appointed by and subject to the direction of the head of the supervisory authority.	6. Each Member State shall ensure that the supervisory authority must have its own staff which shall be appointed by and subject to the direction of the head of the supervisory authority.	6. (…) Member States shall ensure that each supervisory authority must have its own staff which shall (…) be subject to the direction of the member or members of the supervisory authority.	
7. Member States shall ensure that the supervisory authority is subject to financial control which shall not affect its independence. Member States shall ensure that the supervisory authority has separate annual budgets. The budgets shall be made public.	7. Member States shall ensure that the supervisory authority is subject to financial control which shall not affect its independence. Member States shall ensure that the supervisory authority has separate annual budgets. The budgets shall be made public.	7. Member States shall ensure that each supervisory authority is subject to financial control which shall not affect its independence. Member States shall ensure that each supervisory authority has separate, public, annual budgets which may be part of the overall state or national budget.	

Article 41	*Article 41*	*Article 41*	
General conditions for the members of the supervisory authority	***General conditions for the members of the supervisory authority***	***General conditions for the members of the supervisory authority***	
1. Member States shall provide that the members of the supervisory authority must be appointed either by the parliament or the government of the Member State concerned.	1. Member States shall provide that the members of the supervisory authority must be appointed either by the parliament or the government of the Member State concerned.	1. Member States shall provide that the member or members of each supervisory authority must be appointed either by the parliament and/or the government or the head of State of the Member State concerned or by an independent body entrusted by Member State law with the appointment by means of a transparent procedure.	
2. The members shall be chosen from persons whose independence is beyond doubt and whose experience and skills required to perform their duties are demonstrated.	2. The members shall be chosen from persons whose independence is beyond doubt and whose experience and skills required to perform their duties are demonstrated.	2. The member or members shall (…) have the qualifications, experience and skills required to perform their duties and exercise their powers (…).	

3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement in accordance with paragraph 5.	3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement in accordance with paragraph 5.	3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement in accordance with the Member State law.	
4. A member may be dismissed or deprived of the right to a pension or other benefits in its stead by the competent national court, if the member no longer fulfils the conditions required for the performance of the duties or is guilty of serious misconduct.	4. A member may be dismissed or deprived of the right to a pension or other benefits in its stead by the competent national court, if the member no longer fulfils the conditions required for the performance of the duties or is guilty of serious misconduct.	4. deleted	
5. Where the term of office expires or the member resigns, the member shall continue to exercise their duties until a new member is appointed.	5. Where the term of office expires or the member resigns, the member shall continue to exercise their duties until a new member is appointed.	5. deleted	

Article 42	*Article 42*	*Article 42*	
Rules on the establishment of the supervisory authority	***Rules on the establishment of the supervisory authority***	***Rules on the establishment of the supervisory authority***	
Each Member State shall provide by law:	Each Member State shall provide by law:	1. (…) Member States shall provide by law for:	
(a) the establishment and status of the supervisory authority in accordance with Articles 39 and 40;	(a) the establishment and status of the supervisory authority in accordance with Articles 39 and 40;	(a) the establishment (…) of each supervisory authority (…);	
(b) the qualifications, experience and skills required to perform the duties of the members of the supervisory authority;	(b) the qualifications, experience and skills required to perform the duties of the members of the supervisory authority;	(b) the qualifications (…) required to perform the duties of the members of the supervisory authority;	
(c) the rules and procedures for the appointment of the members of the supervisory authority, as well as the rules on actions or occupations incompatible with the duties of the office;	(c) the rules and procedures for the appointment of the members of the supervisory authority, as well as the rules on actions or occupations incompatible with the duties of the office;	(c) the rules and procedures for the appointment of the member or members of each supervisory authority (…);	

(d) the duration of the term of the members of the supervisory authority, which shall be no less than four years, except for the first appointment after entry into force of this Directive, part of which may take place for a shorter period;	(d) the duration of the term of the members of the supervisory authority, which shall be no less than four years, except for the first appointment after entry into force of this Directive, part of which may take place for a shorter period;	(d) the duration of the term of the member or members of each supervisory authority, which shall be no less than four years, except for the first appointment after entry into force of this Directive, part of which may take place for a shorter period where this is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;	
(e) whether the members of the supervisory authority shall be eligible for reappointment;	(e) whether the members of the supervisory authority shall be eligible for reappointment;	(e) whether and, if so, for how many terms, the member or members of each supervisory authority shall be eligible for reappointment;	
(f) the regulations and common conditions governing the duties of the members and staff of the supervisory authority;	(f) the regulations and common conditions governing the duties of the members and staff of the supervisory authority;	(f) the (…) conditions governing the obligations of the member or members and staff of each supervisory authority, prohibitions on actions and occupations incompatible therewith during and after the term of office and rules governing the cessation of employment.	

(g) the rules and procedures on the termination of the duties of the members of the supervisory authority, including where they no longer fulfil the conditions required for the performance of their duties or if they are guilty of serious misconduct.	(g) the rules and procedures on the termination of the duties of the members of the supervisory authority, including where they no longer fulfil the conditions required for the performance of their duties or if they are guilty of serious misconduct.	(g) deleted	
		1a. Member States shall provide that the member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their duties or exercise of their powers.	Moved from Article 43.

Article 43	*Article 43*	*Article 43*	
Professional secrecy	***Professional secrecy***	***Professional secrecy***	
	Amendment 106		
Member States shall provide that the members and the staff of the supervisory authority are subject, both during and after their term of office, 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.	Member States shall provide that the members and the staff of the supervisory authority are subject, both during and after their term of office ***and in conformity with national legislation and practice***, 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***, whilst conducting their duties with independence and transparency as set out in this Directive***.	Moved to Article 42 (1a)	

SECTION 2 DUTIES AND POWERS	SECTION 2 DUTIES AND POWERS	SECTION 2 *TASKS* AND POWERS	
Article 44	***Article 44***	***Article 44***	
Competence	***Competence***	***Competence***	
	Amendment 107		
1. Member States shall provide that each supervisory authority exercises, on the territory of its own Member State, the powers conferred on it in accordance with this Directive.	1. Member States shall provide that each supervisory authority ~~exercises~~***is competent to perform the duties and to exercise***, on the territory of its own Member State, the powers conferred on it in accordance with this Directive.	1. Member States shall provide that each supervisory authority shall be competent on the territory of its own Member State to perform the tasks and exercise the powers conferred on it in accordance with this Directive.	
2. Member States shall provide that the supervisory authority is not competent to supervise processing operations of courts when acting in their judicial capacity.	2. Member States shall provide that the supervisory authority is not competent to supervise processing operations of courts when acting in their judicial capacity.	2. Member States shall provide that the supervisory authority is not competent to supervise processing operations of courts when acting in their judicial capacity. Member States may provide that the supervisory authority is not competent to supervise processing operations of other independent judicial authorities when acting in their judicial capacity.	

Article 45	***Article 45***	***Article 45***	
Duties	***Duties***	***Tasks***	
	Amendment 108		
1. Member States shall provide that the supervisory authority:	1. Member States shall provide that the supervisory authority:	1. Member States shall provide that each supervisory authority shall on its territory:	
(a) monitors and ensures the application of the provisions adopted pursuant to this Directive and its implementing measures;	(a) monitors and ensures the application of the provisions adopted pursuant to this Directive and its implementing measures;	(a) monitor and (…) enforce the application of the provisions adopted pursuant to this Directive and its implementing measures;	
		(aa) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to the processing of personal data;	

		(ab) advise, in accordance with national law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of data subjects' rights and freedoms with regard to the processing of personal data;	
		(ac) promote the awareness of controllers and processors of their obligations under the provisions adopted pursuant to this Directive;	
		(ad) upon request, provide information to any data subject concerning the exercise of his or her rights under the provisions adopted pursuant to this Directive and, if appropriate, co-operate with the supervisory authorities in other Member States to this end;	

(b) hears complaints lodged by any data subject, or by an association representing and duly mandated by that data subject in accordance with Article 50, investigates, to the extent appropriate, the matter and informs the data subject the association of the progress and the outcome of the complaint within a reasonable period, in particular where further investigation or coordination with another supervisory authority is necessary;	(b) hears complaints lodged by any data subject, or by an association ~~representing and duly mandated by that data subject~~ in accordance with Article 50, investigates, to the extent appropriate, the matter and informs the data subject ***or*** the association of the progress and the outcome of the complaint within a reasonable period, in particular where further investigation or coordination with another supervisory authority is necessary;	(b) (…) deal with complaints lodged by (…) data subject, or body, organisation or association representing and duly mandated by a data subject (…), and investigate, to the extent appropriate, the subject matter of the complaint and inform the data subject or the body, organisation or association of the progress and the outcome of the investigation within a reasonable period, in particular where further investigation or coordination with another supervisory authority is necessary;	
(c) checks the lawfulness of data processing pursuant to Article 14, and informs the data subject within a reasonable period on the outcome of the check or on the reasons why the check has not been carried out;	(c) checks the lawfulness of data processing pursuant to Article 14, and informs the data subject within a reasonable period on the outcome of the check or on the reasons why the check has not been carried out;	(c) check the lawfulness of data processing pursuant to Article 15a, and inform the data subject within a reasonable period of the outcome of the check pursuant to Article 15a (3) or on the reasons why the check has not been carried out;	

(d) provides mutual assistance to other supervisory authorities and ensures the consistency of application and enforcement of the provisions adopted pursuant to this Directive;	(d) provides mutual assistance to other supervisory authorities and ensures the consistency of application and enforcement of the provisions adopted pursuant to this Directive;	(d) cooperate with, including sharing information, and provide mutual assistance to other supervisory authorities with a view to ensuring the consistency of application and enforcement of the provisions adopted pursuant to this Directive;	
(e) conducts investigations either on its own initiative or on the basis of a complaint, or on request of another supervisory authority, and informs the data subject concerned, if the data subject has addressed a complaint, of the outcome of the investigations within a reasonable period;	(e) conducts investigations***,*** ***inspections and audits,*** either on its own initiative or on the basis of a complaint, or at the request of another supervisory authority, and informs the data subject concerned, if the data subject has addressed a complaint, of the outcome of the investigations within a reasonable period;	(e) conduct investigations on the application of the provisions adopted pursuant to this Directive (…), including on the basis of a information received from another supervisory or other public authority (…);	
(f) monitors relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies;	(f) monitors relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies;	(f) monitor relevant developments insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies;	

(g) is consulted by Member State institutions and bodies on legislative and administrative measures relating to the protection of individuals' rights and freedoms with regard to the processing of personal data;	(g) is consulted by Member State institutions and bodies on legislative and administrative measures relating to the protection of individuals' rights and freedoms with regard to the processing of personal data;	(g) deleted	
(h) is consulted on processing operations pursuant to Article 26;	(h) is consulted on processing operations pursuant to Article 26;	(h) give advice on processing operations referred to in Article 26;	
(i) participates in the activities of the European Data Protection Board.	(i) participates in the activities of the European Data Protection Board.	(i) contribute to the activities of the European Data Protection Board.	
2. Each supervisory authority shall promote the awareness of the public on risks, rules, safeguards and rights in relation to the processing of personal data. Activities addressed specifically to children shall receive specific attention.	2. Each supervisory authority shall promote the awareness of the public on risks, rules, safeguards and rights in relation to the processing of personal data. Activities addressed specifically to children shall receive specific attention.	2. deleted	
3. The supervisory authority shall, upon request, advise any data subject in exercising the rights laid down in provisions adopted pursuant to this Directive, and, if appropriate, co-operate with the supervisory authorities in other Member States to this end.	3. The supervisory authority shall, upon request, advise any data subject in exercising the rights laid down in provisions adopted pursuant to this Directive, and, if appropriate, co-operate with the supervisory authorities in other Member States to this end.	3. deleted	

4. For complaints referred to in point (b) of paragraph 1, the supervisory authority shall provide a complaint submission form, which can be completed electronically, without excluding other means of communication.	4. For complaints referred to in point (b) of paragraph 1, the supervisory authority shall provide a complaint submission form, which can be completed electronically, without excluding other means of communication.	4. deleted	
5. Member States shall provide that the performance of the duties of the supervisory authority shall be free of charge for the data subject.	5. Member States shall provide that the performance of the duties of the supervisory authority shall be free of charge for the data subject.	5. Member States shall provide that the performance of the (…) tasks of each supervisory authority shall be free of charge for the data subject and for the data protection officer, if any.	
6. Where requests are vexatious, in particular due to their repetitive character, the supervisory authority may charge a fee or not take the action required by the data subject. The supervisory authority shall bear the burden of proving of the vexatious character of the request.	6. Where requests are ~~vexatious~~ ***manifestly excessive***, in particular due to their repetitive character, the supervisory authority may charge a ***reasonable*** fee ~~or not take the action required by the data subject~~. ***Such a fee shall not exceed the costs of taking the action requested.*** The supervisory authority shall bear the burden of proving the ~~vexatious~~ ***manifestly excessive*** character of the request.	6. Member States shall provide that where requests are (…) manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may (…) refuse to act on the request. The supervisory authority shall bear the burden of (…) demonstrating the manifestly unfounded or excessive character of the request.	

Article 46	***Article 46***	***Article 46***	
Powers	***Powers***	***Powers***	
	Amendment 109		
Member States shall provide that each supervisory authority must in particular be endowed with:	***1.*** Member States shall provide that each supervisory authority ~~must in particular be endowed with~~***has the power***:	(1) Each Member State shall provide by law that its supervisory authority shall have effective investigative powers, at least the power to obtain, from the controller and the processor, access to all personal data that is being processed and to all information necessary for the performance of its tasks;	

(a) investigative powers, such as powers of access to data forming the subject matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties;	(a) ~~investigative powers, such as powers of access to data forming the subject matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties~~***to notify the controller or the processor of an alleged breach of the provisions governing the processing of personal data and, where appropriate, order the controller or the processor to remedy that breach, in a specific manner, in order to improve the protection of the data subject;***	Moved to Article 46 (1).	
(b) effective powers of intervention, such as the delivering of opinions before processing is carried out, and ensuring appropriate publication of such opinions, ordering the restriction, erasure or destruction of data, imposing a temporary or definitive ban on processing, warning or	(b) ~~effective powers of intervention, such as the delivering of opinions before processing is carried out, and ensuring appropriate publication of such opinions, ordering the restriction, erasure or destruction of data, imposing a temporary or definitive ban on processing, warning or admonishing the~~	Moved partially to Article 46(1a) (a), (b) and (c) and Article 46(1b)	

admonishing the controller, or referring the matter to national parliaments or other political institutions;	~~controller, or referring the matter to national parliaments or other political institutions~~ ***to order the controller to comply with the data subject's requests to exercise his or her rights under this Directive, including those provided by Articles 12 to 17 where such requests have been refused in breach of those provisions;***		
(c) the power to engage in legal proceedings where the provisions adopted pursuant to this Directive have been infringed or to bring this infringement to the attention of the judicial authorities.	(c) ~~the power to engage in legal proceedings where the provisions adopted pursuant to this Directive have been infringed or to bring this infringement to the attention of the judicial authorities.~~***to order the controller or the processor to provide information pursuant to Article 10(1) and (2) and Articles 11, 28 and 29;***	Moved to Article 46(3)	

	(d) to ensure compliance with opinions on prior consultations referred to in Article 26;		
	(e) to warn or admonish the controller or the processor;		
	(f) to order the rectification, erasure or destruction of all data when they have been processed in breach of the provisions adopted pursuant to this Directive and the notification of such actions to third parties to whom the data have been disclosed;		
	(g) to impose a temporary or definitive ban on processing;		
	(h) to suspend data flows to a recipient in a third country or to an international organisation;		
	(i) to inform national parliaments, the government or other public institutions as well as the public on the matter.		

		(1a) Each Member State shall provide by law that its supervisory authority shall have effective corrective powers such as, for example (a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions adopted pursuant to this Directive; (b) to order the controller or processor to bring processing operations into compliance with the provisions adopted pursuant to this Directive, where appropriate, in a specified manner and within a specified period; in particular by ordering the rectification, restriction or erasure of data pursuant to Article 15; (c) to impose a temporary or definitive limitation on processing.	

		(1b) Each Member State shall provide by law that its supervisory authority shall have the effective advisory powers to advise the controller in accordance with the prior consultation procedure referred to in Article 26 and to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with national law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data.	
	2. Each supervisory authority shall have the investigative power to obtain from the controller or the processor:	2. The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter of Fundamental Rights of the European Union.	

	(a) access to all personal data and to all information necessary for the performance of its supervisory duties, ***(b) access to any of its premises, including to any data processing equipment and means, in accordance with national law, where there are reasonable grounds for presuming that an activity in violation of the provisions adopted pursuant to this Directive is being carried out there, without prejudice to a judicial authorisation if required by national law.***		
	3. Without prejudice to Article 43, Member States shall provide that no additional secrecy requirements shall be issued at the request of supervisory authorities.	3. Each Member State shall provide by law that its supervisory authority shall have the power to (…) bring (…) infringements of provisions adopted pursuant to this Directive *to the attention of judicial* (…) *authorities* and, where appropriate, to commence or *engage* otherwise *in legal proceedings*, in order to enforce the provisions adopted pursuant to this Directive.	Moved from Article 46(1) (c)

	4. Member States may provide that additional security screening in line with national law is required for access to information classified at a level similar to EU CONFIDENTIAL or higher. If no additional security screening is required under the law of the Member State of the relevant supervisory authority, this must be recognised by all other Member States.		
	5. Each supervisory authority shall have the power to bring breaches of the provisions adopted pursuant to this Directive to the attention of the judicial authorities and to engage in legal proceedings and bring an action to the competent court pursuant to Article 53(2).		
	6. Each supervisory authority shall have the power to impose penalties in respect of administrative offences.		

	Amendment 110		
	Article 46a		
	Reporting of breaches		
	1. Member States shall provide that the supervisory authorities take into account guidance issued by the European Data Protection Board pursuant to Article 66(4b) of Regulation (EU) ..../2014 and shall put in place effective mechanisms to encourage confidential reporting of breaches of this Directive.		
	2. Member States shall provide that the competent authorities shall put in place effective mechanisms to encourage confidential reporting of breaches of this Directive.		

Article 47	***Article 47***	***Article 47***	
Activities report	***Activities report***	***Activities report***	
	Amendment 111		
Member States shall provide that each supervisory authority draws up an annual report on its activities. The report shall be made available to the Commission and the European Data Protection Board.	Member States shall provide that each supervisory authority draws up ~~an annual~~ ***a*** report on its activities***, at least every two years***. The report shall be made available to ***the public, the respective Parliament,*** the Commission and the European Data Protection Board. ***It shall include information on the extent to which competent authorities in their jurisdiction have accessed data held by private parties to investigate or prosecute criminal offences***.	Member States shall provide that each supervisory authority draws up an annual report on its activities. The report shall be transmitted to the national parliament, the government and other authorities as designated by national law. It shall be made available to the public, the European Commission and the European Data Protection Board.	

CHAPTER VII CO-OPERATION	CHAPTER VII CO-OPERATION	CHAPTER VII CO-OPERATION	
Article 48	***Article 48***	***Article 48***	
Mutual assistance	***Mutual assistance***	***Mutual assistance***	
	Amendment 112		
1. Member States shall provide that supervisory authorities provide each other with mutual assistance in order to implement and apply the provisions pursuant to this Directive in a consistent manner, and shall put in place measures for effective co-operation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior consultations, inspections and investigations.	1. Member States shall provide that supervisory authorities provide each other with mutual assistance in order to implement and apply the provisions pursuant to this Directive in a consistent manner, and shall put in place measures for effective co-operation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior consultations, inspections and investigations.	1. Member States shall provide that supervisory authorities provide each other with mutual assistance in order to implement and apply the provisions adopted pursuant to this Directive (…) and shall put in place measures for effective co-operation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out (…) inspections and investigations.	

2. Member States shall provide that a supervisory authority takes all appropriate measures required to reply to the request of another supervisory authority.	2. Member States shall provide that a supervisory authority takes all appropriate measures required to reply to the request of another supervisory authority. ***Such measures may include, in particular, the transmission of relevant information or enforcement measures to bring about the cessation or prohibition of processing operations contrary to this Directive without delay and not later than one month after having received the request.***	2. Member States shall provide that a supervisory authority takes all appropriate measures required to reply to the request of another supervisory authority <u>without undue delay and no later than one month after having received the request.</u> (…)	
	2a. The request for assistance shall contain all the necessary information, including the purpose of the request, and reasons for the request. Information exchanged shall be used only in respect of the matter for which it was requested.		
	2b. A supervisory authority to which a request for assistance is addressed may not refuse to comply with it unless:	<u>2b. Member States shall provide that a supervisory authority to which a request for assistance is addressed may not refuse to comply with it unless:</u>	

	(a) it is not competent to deal with the request; or	(a) it is not competent for the subject-matter of the request or for the measures it is requested to execute; or	
	(b) compliance with the request would be incompatible with the provisions adopted pursuant to this Directive.	(b) compliance with the request would be incompatible with the provisions adopted pursuant to this Directive or with Union or Member State law to which the supervisory authority receiving the request is subject.	

3. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress or the measures taken in order to meet the request by the requesting supervisory authority.	3. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress or the measures taken in order to meet the request by the requesting supervisory authority.	3. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress or the measures taken in order to respond to the request. In cases of a refusal under paragraph 2b, it shall explain its reasons for refusing the request.	
	3a. Supervisory authorities shall supply the information requested by other supervisory authorities by electronic means and within the shortest possible period of time, using a standardised format.	3a. Supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means.	
	3b. No fee shall be charged for any action taken following a request for mutual assistance.	3b. No fee shall be charged for any action taken following a request for mutual assistance. Supervisory authorities may agree with other supervisory authorities rules for indemnification by other supervisory authorities for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.	

		3c. The Commission may specify the format and procedures for mutual assistance referred to in this article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 57(2).	
	Amendment 113		
	Article 48a		
	Joint operations		
	1. Member States shall provide that, in order to step up cooperation and mutual assistance, the supervisory authorities may carry out joint enforcement measures and other joint operations in which designated members or staff from supervisory authorities of other Member States participate in operations within a Member State's territory.		

	2. Member States shall provide that in cases where data subjects in another Member State or other Member States are likely to be affected by processing operations, the competent supervisory authority may be invited to participate in the joint operations. The competent supervisory authority may invite the supervisory authority of each of those Member States to take part in the respective operation and in case where it is invited, respond to the request of a supervisory authority to participate in the operations without delay.		
	3. Member States shall lay down the practical aspects of specific co-operation actions.		

Article 49	*Article 49*	*Article 49*	
Tasks of the European Data Protection Board	***Tasks of the European Data Protection Board***	***Tasks of the European Data Protection Board***	
	Amendment 114		
1. The European Data Protection Board established by Regulation (EU)…./2012 shall exercise the following tasks in relation to processing within the scope of this Directive:	1. The European Data Protection Board established by Regulation (EU)…./~~2012~~***2014*** shall exercise the following tasks in relation to processing within the scope of this Directive:	1. The European Data Protection Board established by Regulation (EU)…./ XXX exercise the following tasks in relation to processing within the scope of this Directive:	
(a) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Directive;	(a) advise the ~~Commission~~***Union institutions*** on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Directive;	(a) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Directive;	

(b) examine, on request of the Commission or on its own initiative or of one of its members, any question covering the application of the provisions adopted pursuant to this Directive and issue guidelines, recommendations and best practices addressed to the supervisory authorities in order to encourage consistent application of those provisions;	(b) examine, ~~on~~***at the*** request of the Commission***, the European Parliament or the Council*** or on its own initiative or of one of its members, any question covering the application of the provisions adopted pursuant to this Directive and issue guidelines, recommendations and best practices addressed to the supervisory authorities in order to encourage consistent application of those provisions***, including on the use of enforcement powers***;	(b) examine, on its own initiative or on request of one of its members or on request of the Commission, any question covering the application of the provisions adopted pursuant to this Directive and issue guidelines, recommendations and best practices (…) in order to encourage consistent application of those provisions;	
		(ba) draw up guidelines for supervisory authorities concerning the application of measures referred to in paragraph 1 and 1b of Article 46;	
(c) review the practical application of guidelines, recommendations and best practices referred to in point (b) and report regularly to the Commission on these;	(c) review the practical application of guidelines, recommendations and best practices referred to in point (b) and report regularly to the Commission on these;	(c) review the practical application of the guidelines, recommendations and best practices referred to in point (b) and ba;	

(d) give the Commission an opinion on the level of protection in third countries or international organisations;	(d) give the Commission an opinion on the level of protection in third countries or international organisations;	(d) give the Commission an opinion on the level of protection in third countries or international organisations;	
(e) promote the co-operation and the effective bilateral and multilateral exchange of information and practices between the supervisory authorities;	(e) promote the co-operation and the effective bilateral and multilateral exchange of information and practices between the supervisory authorities***, including the coordination of joint operations and other joint activities where it so decides at the request of one or more supervisory authorities***;	(e) promote the co-operation and the effective bilateral and multilateral exchange of information and practices between the supervisory authorities;	
(f) promote common training programmes and facilitate personnel exchanges between the supervisory authorities, as well as, where appropriate, with the supervisory authorities of third countries or of international organisations;	(f) promote common training programmes and facilitate personnel exchanges between the supervisory authorities, as well as, where appropriate, with the supervisory authorities of third countries or of international organisations;	(f) promote common training programmes and facilitate personnel exchanges between the supervisory authorities, as well as, where appropriate, with the supervisory authorities of third countries or of international organisations;	

(g) promote the exchange of knowledge and documentation with data protection supervisory authorities worldwide, including data protection legislation and practice.	(g) promote the exchange of knowledge and documentation with data protection supervisory authorities worldwide, including data protection legislation and practice~~.~~***;***	(g) promote the exchange of knowledge and documentation <u>on data protection legislation and practice</u> with data protection supervisory authorities worldwide.	
	(ga) give its opinion to the Commission in the preparation of delegated and implementing acts under this Directive.		
2. Where the Commission requests advice from the European Data Protection Board, it may lay out a time limit within which the European Data Protection Board shall provide such advice, taking into account the urgency of the matter.	2. Where ***the European Parliament, the Council or*** the Commission requests advice from the European Data Protection Board, it may lay out a time limit within which the European Data Protection Board shall provide such advice, taking into account the urgency of the matter.	2. Where the Commission requests advice from the European Data Protection Board, it may <u>indicate</u> a time limit (…) taking into account the urgency of the matter.	

3. The European Data Protection Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 57(1) and make them public.	3. The European Data Protection Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 57(1) and make them public.	3. The European Data Protection Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 57(1) and make them public.	
4. The Commission shall inform the European Data Protection Board of the action it has taken following opinions, guidelines, recommendations and best practices issued by the European Data Protection Board.	4. The Commission shall inform the European Data Protection Board of the action it has taken following opinions, guidelines, recommendations and best practices issued by the European Data Protection Board.	4. The Commission shall inform the European Data Protection Board of the action it has taken following opinions, guidelines, recommendations and best practices issued by the European Data Protection Board.	

CHAPTER VIII REMEDIES, LIABILITY AND SANCTIONS	CHAPTER VIII REMEDIES, LIABILITY AND SANCTIONS	CHAPTER VIII REMEDIES, LIABILITY AND SANCTIONS	
Article 50	***Article 50***	***Article 50***	
Right to lodge a complaint with a supervisory authority	***Right to lodge a complaint with a supervisory authority***	***Right to lodge a complaint with a supervisory authority***	
	Amendment 115		
1. Without prejudice to any other administrative or judicial remedy, Member States shall provide for the right of every data subject to lodge a complaint with a supervisory authority in any Member State, if they consider that the processing of personal data relating to them does not comply with provisions adopted pursuant to this Directive.	1. Without prejudice to any other administrative or judicial remedy, Member States shall provide for the right of every data subject to lodge a complaint with a supervisory authority in any Member State, if they consider that the processing of personal data relating to them does not comply with provisions adopted pursuant to this Directive.	1. Without prejudice to any other administrative or judicial remedy, Member States shall provide that every data subject shall have the right to lodge a complaint with a single supervisory authority, (…) if the data subject considers that the processing of personal data relating to him or her does not comply with provisions adopted pursuant to this Directive.	

		1a. Member States shall provide that if the complaint is not lodged with the supervisory authority that is competent pursuant to Article 44 (1), the supervisory authority with which the complaint has been lodged shall transmit it to the competent supervisory authority, without undue delay. The data subject shall be informed about the transmission.	
		1b. Member States shall provide that the supervisory authority with which the complaint has been lodged provides further assistance upon the request of the data subject.	
2. Member States shall provide for the right of any body, organisation or association which aims to protect data subjects' rights and interests concerning the protection of their personal data and is being properly constituted according to the law of a Member State to lodge a complaint with a supervisory authority in any Member State on	2. Member States shall provide for the right of any body, organisation or association ***acting in the public interest*** which ~~aims to protect data subjects' rights and interests concerning the protection of their personal data and is being which~~ ***has been*** properly constituted according to the law of a Member State to lodge a complaint with a	2. Moved to Article 53.	

behalf of one or more data subjects, if it considers that a data subject's rights under this Directive have been infringed as a result of the processing of personal data. The organisation or association must be duly mandated by the data subject(s).	supervisory authority in any Member State on behalf of one or more data subjects, if it considers that a data subject's rights under this Directive have been infringed as a result of the processing of personal data. ~~The organisation or association must be duly mandated by the data subject(s).~~		
		2a. The data subject shall be informed by the competent supervisory authority of the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 51.	
3. Member States shall provide for the right of any body, organisation or association referred to in paragraph 2, independently of a data subject's complaint, to lodge a complaint with a supervisory authority in any Member State, if it considers that a personal data breach has occurred.	3. Member States shall provide for the right of any body, organisation or association referred to in paragraph 2, independently of a data subject's complaint, to lodge a complaint with a supervisory authority in any Member State, if it considers that a personal data breach has occurred.	3. deleted	

Article 51	*Article 51*	*Article 51*	
Right to a judicial remedy against a supervisory authority	***Right to a judicial remedy against a supervisory authority***	***Right to a judicial remedy against a supervisory authority***	
	Amendment 116		
1. Member States shall provide for the right to a judicial remedy against decisions of a supervisory authority.	1. Member States shall provide for the right ***for each natural or legal person*** to a judicial remedy against decisions of a supervisory authority ***concerning them***.	1. Without prejudice to any other administrative or non-judicial remedy, Member States shall provide for the right of a natural or legal person to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.	
2. Each data subject shall have the right to a judicial remedy for obliging the supervisory authority to act on a complaint, in the absence of a decision which is necessary to protect their rights, or where the supervisory authority does not inform the data subject within three months on the progress or outcome of the complaint pursuant to point (b) of Article 45(1).	2. ***Member States shall provide that*** ~~Each~~***each*** data subject shall have the right to a judicial remedy for obliging the supervisory authority to act on a complaint, in the absence of a decision which is necessary to protect their rights, or where the supervisory authority does not inform the data subject within three months on the progress or outcome of the complaint pursuant to point (b) of Article 45(1).	2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the supervisory authority competent in accordance with Article 44 (1) does not deal with the complaint (…) or does not inform the data subject within three months or any shorter period provided under Union or Member States law on the progress or outcome of the complaint lodged under Article 50.	

3. Member States shall provide that proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.	3. Member States shall provide that proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.	3. Member States shall provide that proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.	
	3a. Member States shall ensure that final decisions by the court referred to in this Article will be enforced.		

Article 52	***Article 52***	***Article 52***	
Right to a judicial remedy against a controller or processor	***Right to a judicial remedy against a controller or processor***	***Right to a judicial remedy against a controller or processor***	
	Amendment 117		
Without prejudice to any available administrative remedy, including the right to lodge a complaint with a supervisory authority, Member States shall provide for the right of every natural person to a judicial remedy if they consider that that their rights laid down in provisions adopted pursuant to this Directive have been infringed as a result of the processing of their personal data in non-compliance with these provisions.	***1.*** Without prejudice to any available administrative remedy, including the right to lodge a complaint with a supervisory authority, Member States shall provide for the right of every natural person to a judicial remedy if they consider that that their rights laid down in provisions adopted pursuant to this Directive have been infringed as a result of the processing of their personal data in non-compliance with these provisions.	Without prejudice to any available administrative <u>or non-judicial</u> remedy, including the right to lodge a complaint with a supervisory authority <u>under Article 50</u>, Member States shall provide for the right of <u>data subjects</u> to a<u>n effective</u> judicial remedy if they consider that their rights laid down in provisions adopted pursuant to this Directive have been infringed as a result of the processing of their personal data in non-compliance with these provisions.	
	1a. Member States shall ensure that final decisions by the court referred to in this Article will be enforced.		

Article 53	***Article 53***	***Article 53***	
Common rules for court proceedings	***Common rules for court proceedings***	***(…) Representation of data subjects***	
	Amendment 118		
1. Member States shall provide for the right of any body, organisation or association referred to in Article 50(2) to exercise the rights referred to in Articles 51 and 52 on behalf of one or more data subjects.	1. Member States shall provide for the right of any body, organisation or association referred to in Article 50(2) to exercise the rights referred to in Articles 51**,** ~~and~~ 52 ~~on behalf of~~ ***and 54 when mandated by*** one or more data subjects.	*Member States shall*, in accordance with national procedural law, provide that the data subject shall have the right to mandate a *body, organisation or association, which has been properly constituted according to the law of a Member State* and whose statutory objectives include the protection of *data subjects' rights and* freedoms with regard to the *protection of their personal data, to lodge* the *complaint* on his or her behalf and to exercise the rights referred to in Articles 50, 51 and 52 on his or her behalf.	Moved from Article 50.

	Amendment 119		
2. Each supervisory authority shall have the right to engage in legal proceedings and bring an action to court, in order to enforce the provisions adopted pursuant to this Directive or to ensure consistency of the protection of personal data within the Union.	2. ***Member States shall provide that*** ~~Each~~ ***each*** supervisory authority shall have the right to engage in legal proceedings and bring an action to court, in order to enforce the provisions adopted pursuant to this Directive or to ensure consistency of the protection of personal data within the Union.	2. deleted	
3. Member States shall ensure that court actions available under national law allow for the rapid adoption of measures including interim measures, designed to terminate any alleged infringement and to prevent any further impairment of the interests involved.	3. Member States shall ensure that court actions available under national law allow for the rapid adoption of measures including interim measures, designed to terminate any alleged infringement and to prevent any further impairment of the interests involved.	3. deleted	

Article 54	*Article 54*	*Article 54*	
Liability and the right to compensation	***Liability and the right to compensation***	***(…) Right to compensation (…)***	
	Amendment 120		
1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with the provisions adopted pursuant to this Directive shall have the right to receive compensation from the controller or the processor for the damage suffered.	1. Member States shall provide that any person who has suffered damage***, including non pecuniary damage,*** as a result of an unlawful processing operation or of an action incompatible with the provisions adopted pursuant to this Directive shall have the right to ~~receive~~ ***claim*** compensation from the controller or the processor for the damage suffered.	1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive shall be entitled to receive compensation for the damage suffered from the controller or any other authority competent under national law.	
2. Where more than one controller or processor is involved in the processing, each controller or processor shall be jointly and severally liable for the entire amount of the damage.	2. Where more than one controller or processor is involved in the processing, each controller or processor shall be jointly and severally liable for the entire amount of the damage.	2. deleted	

3. The controller or the processor may be exempted from this liability, in whole or in part, if the controller or processor proves that they are not responsible for the event giving rise to the damage.	3. The controller or the processor may be exempted from this liability, in whole or in part, if the controller or processor proves that he or she is not responsible for the event giving rise to the damage.	3. deleted	
Article 55	***Article 55***	***Article 55***	
Penalties	***Penalties***	***Penalties***	
Member States shall lay down the rules on penalties, applicable to infringements of the provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for must be effective, proportionate and dissuasive.	Member States shall lay down the rules on penalties, applicable to infringements of the provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for must be effective, proportionate and dissuasive.	Member States shall lay down the rules on penalties, applicable to infringements of the provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for must be effective, proportionate and dissuasive.	

	Amendment 121		
	CHAPTER VIIIa TRANSMISSION OF PERSONAL DATA TO THIRD PARTIES		
	Article 55a		
	Transmission of personal data to other authorities or private parties in the Union		
	1. Member States shall ensure that the controller does not transmit or instruct the processor to transmit personal data to a natural or legal person not subject to the provisions adopted pursuant to this Directive, unless:		
	(a) the transmission complies with Union or Member State law; and		
	(b) the recipient is established in a Member State of the European Union; and		

	(c) no legitimate specific interests of the data subject prevent transmission; and		
	(d) the transmission is necessary in a specific case for the controller transmitting the personal data for:		
	(i) the performance of a task lawfully assigned to it; or		
	(ii) the prevention of an immediate and serious danger to public security; or		
	(iii) the prevention of serious harm to the rights of individuals.		
	2. The controller shall inform the recipient of the purpose for which the personal data may exclusively be processed.		

	3. The controller shall inform the supervisory authority of such transmissions.		
	4. The controller shall inform the recipient of processing restrictions and ensure that those restrictions are met.		

CHAPTER IX DELEGATED ACTS AND IMPLEMENTING ACTS	CHAPTER IX DELEGATED ACTS AND IMPLEMENTING ACTS	CHAPTER IX (…) IMPLEMENTING ACTS	
Article 56	***Article 56***	***Article 56***	
Exercise of the delegation	***Exercise of the delegation***	***Exercise of the delegation***	
	Amendment 122		
1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.	1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.	deleted	
2. The delegation of power referred to in Article 28(5) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Directive.	2. The ~~delegation of power~~***power to adopt delegated acts*** referred to in ***Article 25a(7),*** Article 28(5)***, Article 34(3) and Article 34(5)*** shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Directive.	2. deleted	

3. The delegation of power referred to in Article 28(5) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.	3. The delegation of power referred to in ***Article 25a(7),*** Article 28(5)***, Article 34(3) and Article 34(5)*** may be revoked at any time by the European Parliament or by the Council. A decision ~~of revocation~~ ***to revoke*** shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.	3. deleted	
4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.	4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.	4. deleted	

5. A delegated act adopted pursuant to Article 28(5) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of 2 months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by 2 months at the initiative of the European Parliament or the Council.	5. A delegated act adopted pursuant to ***Article 25a(7),*** Article 28(5)***, Article 34(3) and Article 34(5)*** shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of ~~2~~***six*** months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by ~~2~~***six*** months at the initiative of the European Parliament or ***of*** the Council.	5. deleted	
	Amendment 123		
	Article 56a		
	Deadline for the adoption of delegated acts		
	The Commission shall adopt the delegated acts under Article 25a(7) and Article 28(5) by [six months before the date referred to in Article 62(1)]. The Commission may extend the deadline referred to in this paragraph by six months.		

Article 57	***Article 57***	***Article 57***	
Committee procedure	***Committee procedure***	***Committee procedure***	
	Amendment 124		
1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.	1. The Commission shall be assisted by a committee. 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 87 of Regulation (EU) XXX. 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.	
3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.	***deleted***	3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.	

CHAPTER X FINAL PROVISIONS	CHAPTER X FINAL PROVISIONS	CHAPTER X FINAL PROVISIONS	
Article 58	***Article 58***	***Article 58***	
Repeals	***Repeals***	***Repeals***	
1. Council Framework Decision 2008/977/JHA is repealed.	1. Framework Decision 2008/977/JHA is repealed.	1. Council Framework Decision 2008/977/JHA is repealed with effect from the date referred to in Article 62(1).	
2. References to the repealed Framework Decision referred to in paragraph 1 shall be construed as references to this Directive.	2. References to the repealed Framework Decision referred to in paragraph 1 shall be construed as references to this Directive.	2. References to the repealed Framework Decision referred to in paragraph 1 shall be construed as references to this Directive.	

Article 59	*Article 59*	*Article 59*	
Relation with previously adopted acts of the Union for judicial co-operation in criminal matters and police co-operation	***Relation with previously adopted acts of the Union for judicial co-operation in criminal matters and police co-operation***	***Relation<u>ship</u> with previously adopted acts of the Union for judicial co-operation in criminal matters and police co-operation***	
The specific provisions for the protection of personal data with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties in acts of the Union adopted prior to the date of adoption of this Directive regulating the processing of personal data between Member States and the access of designated authorities of Member States to information systems established pursuant to the Treaties within the scope of this Directive remain unaffected.	The specific provisions for the protection of personal data with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties in acts of the Union adopted prior to the date of adoption of this Directive regulating the processing of personal data between Member States and the access of designated authorities of Member States to information systems established pursuant to the Treaties within the scope of this Directive remain unaffected.	The specific provisions for the protection of personal data <u>in acts of the Union adopted in the field of judicial co-operation in criminal matters and police co-operation</u> (…) adopted prior to the date of adoption of this Directive regulating the processing of personal data between Member States and the access of designated authorities of Member States to information systems established pursuant to the Treaties within the scope of this Directive remain unaffected.	

Article 60	*Article 60*	*Article 60*	
Relationship with previously concluded international agreements in the field of judicial co-operation in criminal matters and police co-operation	***Relationship with previously concluded international agreements in the field of judicial co-operation in criminal matters and police co-operation***	***Relationship with previously concluded international agreements in the field of judicial co-operation in criminal matters and police co-operation***	
International agreements concluded by Member States prior to the entry force of this Directive shall be amended, where necessary, within five years after the entry into force of this Directive.	International agreements concluded by Member States prior to the entry force of this Directive shall be amended, where necessary, within five years after the entry into force of this Directive.	International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to the entry into force of this Directive and which are in compliance with Union law applicable prior to the entry into force of this Directive shall remain in force until amended, replaced or revoked.	

Article 61	***Article 61***	***Article 61***	
Evaluation	***Evaluation***	***Evaluation***	
	Amendment 125		
1. The Commission shall evaluate the application of this Directive.	1. The Commission shall***, after requesting an opinion of the European Data Protection Board,*** evaluate the application ***and implementation*** of this Directive. ***It shall coordinate in close cooperation with the Member States and shall include announced and unannounced visits. The European Parliament and the Council shall be kept informed throughout the process and shall have access to the relevant documents.***	1. The Commission shall evaluate the application of this Directive. In the context of this evaluation the Commission shall examine, in particular, the application and functioning of the provisions of Article 36aa.	

2. The Commission shall review within three years after the entry into force of this Directive other acts adopted by the European Union which regulate the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, in particular those acts adopted by the Union referred to in Article 59, in order to assess the need to align them with this Directive and make, where appropriate, the necessary proposals to amend these acts to ensure a consistent approach on the protection of personal data within the scope of this Directive.	2. The Commission shall review within ~~three~~ ***two*** years after the entry into force of this Directive other acts adopted by the European Union which regulate the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, in particular those acts adopted by the Union referred to in Article 59, ~~in order to assess the need to align them with this Directive and make, where appropriate, the necessary proposals to amend these acts to ensure a consistent approach on the protection of personal data~~ ***and shall make appropriate proposals with a view to ensuring consistent and homogeneous legal rules relating to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties*** within the scope of this Directive.	2. The Commission shall review within five years after the entry into force of this Directive other acts adopted by the European Union which regulate the processing of personal data by the competent authorities for the purposes (…) set out in Article 1(1) including those acts adopted by the Union referred to in Article 59, in order to assess the need to align them with this Directive and make, where appropriate, the necessary proposals to amend these acts to ensure a consistent approach on the protection of personal data within the scope of this Directive.	

	2a. The Commission shall present within two years of the entry into force of this Directive appropriate proposals for the revision of the legal framework applicable to the processing of personal data by Union institutions, bodies, offices and agencies, for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties with a view to ensuring consistent and homogeneous legal rules relating to the fundamental right to the protection of personal data in the Union.		

3. The Commission shall submit reports on the evaluation and review of this Directive pursuant to paragraph 1 to the European Parliament and the Council at regular intervals. The first reports shall be submitted no later than four years after the entry into force of this Directive. Subsequent reports shall be submitted every four years thereafter. The Commission shall submit, if necessary, appropriate proposals with a view of amending this Directive and aligning other legal instruments. The report shall be made public.	3. The Commission shall submit reports on the evaluation and review of this Directive pursuant to paragraph 1 to the European Parliament and ***to*** the Council at regular intervals. The first reports shall be submitted not later than four years after the entry into force of this Directive. Subsequent reports shall be submitted every four years thereafter. The Commission shall submit, if necessary, appropriate proposals with a view to amending this Directive and aligning other legal instruments. The report shall be made public.	3. The Commission shall submit reports on the evaluation and review of this Directive pursuant to paragraph 1 to the European Parliament and the Council at regular intervals. The first reports shall be submitted no later than four years after the entry into force of this Directive. Subsequent reports shall be submitted every four years thereafter. The Commission shall submit, if necessary, appropriate proposals with a view of amending this Directive and aligning other legal instruments. The report shall be made public.	

Article 62	*Article 62*	*Article 62*	
Implementation	***Implementation***	***Implementation***	
1. Member States shall adopt and publish, by [date/ two years after entry into force] at the latest, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall forthwith notify to the Commission the text of those provisions.	1. Member States shall adopt and publish, by …* at the latest, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall forthwith notify to the Commission the text of those provisions. ****OJ: please insert the date: two years after the date of entry into force of this Directive.***	1. Member States shall adopt and publish, by [date/ three years after entry into force] at the latest, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall forthwith notify to the Commission the text of those provisions.	
They shall apply those provisions from xx.xx.201x [date/ two years after entry into force].	They shall apply those provisions from …* ****OJ: please insert the date: two years after the date of entry into force of this Directive.***	They shall apply those provisions from xx.xx.201x [date/ three years after entry into force].	
When Member States adopt those provisions, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.	When Member States adopt those provisions, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.	When Member States adopt those provisions, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.	

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.	2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.	2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive	
Article 63	***Article 63***	***Article 63***	
Entry into force and application	***Entry into force and application***	***Entry into force (…)***	
This Directive shall enter into force on the first day following that of its publication in the Official Journal of the European Union.	This Directive shall enter into force on the first day following that of its publication in the *Official Journal of the European Union*.	This Directive shall enter into force on the first day following that of its publication in the Official Journal of the European Union.	
Article 64	***Article 64***	***Article 64***	
Addressees	***Addressees***	***Addressees***	
This Directive is addressed to the Member States.	This Directive is addressed to the Member States.	This Directive is addressed to the Member States.	
Done at Brussels, 25.1.2012	Done at …,	Done at …,	
For the European Parliament *The President*	*For the European Parliament* *The President*	*For the European Parliament* *The President*	
For the Council *The President*	*For the Council* *The President*	*For the Council* *The President*	