Council of the European Union

Brussels, 13 November 2014
(OR. en)

15389/14

LIMITE

DATAPROTECT 163
JAI 858
MI 873
DRS 149
DAPIX 165
FREMP 200
COMIX 602
CODEC 2220

Interinstitutional File:
2012/0011 (COD)

NOTE

From:	Presidency
To:	COREPER
Subject:	Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [First reading] - Public sector = Partial General approach

I. Introduction

1. The purpose of this Presidency note is to prepare the Council discussion at the JHA Council meeting in December 2014 on the inclusion of the public sector in the scope of the draft General Data Protection Regulation (hereinafter referred to as the 'GDPR') and the leeway that Member States should be given in this regard.

   Chapter IX of the GDPR, which provides for a number of specific data protection regimes for specific types of processing, will also be submitted to the December Council for a partial general approach. This Chapter will be the subject of a later note to CRP.

2. The question whether and how to deal with processing of personal data by the public sector in the draft General Data Protection Regulation (GDPR) is one of particular sensitivity and importance to delegations. It was already debated at the JHA Informal Ministerial Meeting in Nicosia in July 2012 and at the JHA Council meetings in October and December 2012. At the latter Council meeting it was decided that the question as to whether and how the Regulation could provide flexibility for the Member States' public sector, would be decided following completion of the first examination of the text of the GDPR. More recently, at the informal Ministerial Meeting in Milan on 9 July 2014 an overall majority of Member States supported a Regulation as legal instrument, but the need to provide Member States with sufficient leeway to determine the data protection requirements applicable to the public sector was equally emphasised.

II. Legislative techniques used to take account of the public sector

3. The specificity of the public sector has been taken into account during the examination of the GDPR by tailoring some data protection rules to the specific needs of the public sector. The draft GDPR now contains a significant number of provisions which are specifically tailored to the needs of public authorities and bodies in their capacities as controllers or processors. In some instances application to the public sector has been excluded (e.g. the right to data portability or the right to be forgotten). The principle of public access to official documents was also taken expressly into account.

4. Apart from these specific amendments, three different elements have been used in the Regulation to offer a certain leeway to the Member States' public sector to modulate the requirements of the Regulation in accordance with specificities of their constitutional, legal and institutional set-up.

a. ***Detailing the scope of national law as a legal basis for data processing***

5. First, the Regulation does not require Member States to abrogate specific data protection laws in the public sector. On the contrary, it allows Member States to specify the rules of the Regulation for certain areas of the public sector. The current wording of Article 6 (3) indicates what type of details may be specified by national or Union law in order to ensure the appropriate level of protection.

b. Restricting data protection rights and obligations by national law

6. Secondly, Article 21 allows Member States to restrict certain rights and obligations through national law provided such restrictions constitute a necessary and proportionate measure in a democratic society to safeguard a number of public interests as well as the protection of the data subject and the rights and freedoms of others.

c. Specific data protection regimes

7. Thirdly, Chapter IX of the GDPR provides for a number of specific data protection regimes for specific types of processing. This Chapter, which will be the subject of a later note, will also be submitted to the December Council for a partial general approach.

III. Question to Council

8. Against this background and further to the Informal Ministerial Meeting on 9 July 2014 in Milan, the Presidency had invited the Working Party on Information Exchange and Data Protection (DAPIX) to express itself on the following elements:

   a) the need for a minimum harmonisation clause for the public sector; and

   b) the need for further detailing the legislative powers of Member States in case processing is necessary for compliance with a legal obligation or necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

a. Allow Member States to provide for a higher level of protection: minimum harmonisation for the public sector

9. The GDPR seeks to replace the 1995 Data Protection Directive[1]. The choice of a Regulation as the legal instrument to replace a Directive is motivated by the goal to create a level playing field in terms of data protection legislation. This level playing field implies primarily that the rights of data subjects and the corresponding obligations of controllers regarding the protection of personal data are identical in all Member States. This goal already underlies the current Data Protection Directive, which is aimed at establishing an equivalent level of protection in all Member States (recital 8) and which, according to the ECJ, should be interpreted as seeking to generally achieve complete harmonisation[2]. This implies that the obligations in the Directive to protect personal data constitute both the minimum and maximum level of protection that Member States may impose in this regard.

10. Some delegations have argued that this goal is less relevant with regard to personal data which are collected and further processed by public authorities or bodies in the exercise of their public duties. Some Member States have therefore expressed their support for a minimum harmonisation clause for the public sector, which would allow them to adopt data protection legislation providing *a higher level of protection* than the one of the Regulation. They have argued that allowing Member States to provide for a higher level of protection under national law coupled with a free movement clause would be in line with the changed legal basis (Article 16 TFEU). The Framework Decision of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters already contains a minimum harmonisation clause[3].

1 OJ L 281, 23.11.1995, p. 31.
2 ECJ, Lindqvist, C 101/01, judgment of 6 November 2003, paragraph 96.
3 It explicitly states it that it does not 'preclude Member States from providing, for the protection of personal data collected or processed at national level, higher safeguards than those established in [the] Framework Decision' (Article 1(5)).

11. The Commission, on the other hand, argues that EU citizens are entitled to expect similar levels of data protection in the public sector in Member States, given that the fundamental right to data protection does not differentiate between the public and private sector. Another argument from the Commission is that harmonisation in this area is also necessary as cross-border exchange of data is increasing between public authorities. Indeed, if authorities in different Member States applied different data protection standards this could constitute an obstacle to the exchange of information between those authorities. However, the free movement of data as required by Article 16 TFEU would be ensured by the free movement clause in Article 1(3) of the draft Regulation[4].

b. ***Clarify the legislative powers of Member States and allow them to derogate from the Regulation in the public interest***

12. At the October DAPIX meetings, a majority of Member States appeared to be of the opinion that the need to take account of the constitutional, legal and political specificities of the public sector in each Member State can be sufficiently accommodated by clarifying the legislative powers that Member States have when processing of personal data is carried out on the legal bases referred to in paragraphs (c) and (e) of Article 6, i.e. to ensure compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. This allows Member States to adopt more specific laws as far as there is no contradiction with the Regulation. The Presidency has therefore introduced these clarifications in paragraph 3 of Article 6 (which applies to processing both in the public and private sector), as well as in paragraph 2a of Article 1. This allows Member States to *specify and adapt national data protection laws to the specificities of the public sector*, while barring them from adopting laws that provide for a higher level of protection than that of the Regulation.

---

[4] Contrary to the situation in the case of private entities there is, however, no "free" flow of personal data between public authorities. They may exchange personal data only when expressly authorised to do so. Various EU sectoral instruments (e.g. in the field of health, banking and financial markets supervision, agriculture, taxation or social security) have regulated the conditions that Member States may attach to the exchange of information, including personal data, between their authorities. These conditions vary in nature and many of them are not linked to data protection concerns. Even if the GDPR were to be adopted as proposed by the Commission, these sectoral EU rules would continue to apply (*lex specialis*).

13. Moreover, Article 21 allows Member States to derogate from certain requirements of the Regulation by adopting legislative measures, provided such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties as well as other important objectives of general public interests of the Union or of a Member State[5] and the protection of the data subject or the rights and freedoms of others. This is, in fact, a traditional human rights clause based on the necessity and proportionality tests[6] which allows certain justified limitations to the protected fundamental right. While this applies both to the private and public sector, it is more relevant for personal data processed by public authorities. As in the case of Article 6(3), Article 21 does not allow a Member State to lay down a higher level of data protection.

14. *Delegations are invited to confirm that they are satisfied that the solutions currently provided for in Articles 1(2a), 6(3) and 21will allow them to take sufficient account of the specificities of the public sector in the application of the future GDPR*.

---

[5] Article 21 refers to 'important economic or financial interest of the Union or of a Member State, including, monetary, budgetary and taxation matters, public health and social security, the protection of market stability and integrity', 'the performance of a task assigned to courts under Union or Member State law to be carried out independently', was well as 'the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions', 'the monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority'.

[6] This in line with Article 52 of the Charter of Fundamental Rights of the European Union.

…….

7) The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the way data protection is implemented across the Union, legal uncertainty and a widespread public perception that there are significant risks for the protection of individuals associated notably with online activity. Differences in the level of protection of the rights and freedoms of individuals, notably to the right to the protection of personal data, with regard to the processing of personal data afforded in the Member States may prevent the free flow of personal data throughout the Union. These differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. This difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC.

8) In order to ensure a consistent and high level of protection of individuals and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of individuals with regard to the processing of such data should 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. Regarding the processing of personal data by public authorities for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed **to** maintain or introduce national provisions **to further specify the application of the rules of this Regulation**, except for those cases where this Regulation lays down specific regimes of data protection.

9) Effective protection of personal data throughout the Union requires strengthening and detailing the rights of data subjects and the obligations of those who process and determine the processing of personal data, but also equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent **sanctions** for offenders in the Member States.

10) Article 16(2) of the Treaty 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.

11) In order to ensure a consistent level of protection for individuals throughout the Union and to prevent divergences hampering the free movement of data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide individuals in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors or at least the same minimum level of legally enforceable rights and obligations and responsibilities regarding the processing of personal data by public **bodies** for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, to ensure consistent monitoring of the processing of personal data, and equivalent **sanctions** in all Member States as well as effective co-operation by the supervisory authorities of different Member States. The proper functioning of the internal market requires that the free movement of personal data within the Union should not be restricted or prohibited for reasons connected with the protection of individuals with regard to the processing of personal data. When Member States maintain or introduce (…) national provisions **specifying application of the rules of this Regulation** regarding the processing of personal data by their public **bodies** performing a task carried out in the public interest or in the exercise of official authority vested in the controller, they should not be allowed to impose other requirements than those flowing from this Regulation regarding data provided by public authorities from another Member State nor should they be allowed to impose any other requirements than those flowing from this Regulation regarding personal data they provide to public authorities from another Member State.

To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a number of derogations. In addition, the Union institutions and bodies, Member States and their supervisory authorities are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. The notion of micro, small and medium-sized enterprises should draw upon Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises.

12) The protection afforded by this Regulation concerns natural persons, whatever their nationality or place of residence, in relation to the processing of personal data. With regard to the processing of data which concern legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person, the protection of this Regulation should not be claimed by any such person. (…).

13) The protection of individuals should be technologically 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 Regulation.

14) This Regulation does not address issues of protection of fundamental rights and freedoms or the free flow of data related to activities which fall outside the scope of Union law, such as activities concerning national security, taking into account Articles 3 to 6 of the Treaty on the Functioning of the European Union (…) nor does it cover the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.

14a) Regulation (EC) No 45/2001[7] 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 this Regulation.

15) This Regulation should not apply to processing of personal data by a natural person in the course of a personal or household activity, and thus without a connection with a professional or commercial activity. Personal and household activities include social networking and on-line activity undertaken within the context of such personal and household activities. However, this Regulation should (…) apply to controllers or processors which provide the means for processing personal data for such personal or domestic activities.

16) 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, and, for these purposes, the maintenance of public order, or the execution of criminal penalties and the free movement of such data, is subject of a specific legal instrument at Union level. Therefore, this Regulation should not apply to the processing activities for those purposes. However, data processed by public authorities under this Regulation when used for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties should be governed by the more specific legal instrument at Union level (Directive XX/YYY).

When processing of personal data by (...) private bodies falls within the scope of this Regulation, this Regulation should provide for the possibility for Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific important interests including public security and the prevention, investigation, detection and prosecution of criminal offences. This is relevant for instance in the framework of anti-money laundering or the activities of forensic laboratories.

[7] OJ L 8, 12.1.2001, p. 1.

16a) *While this Regulation applies also to the activities of courts* and other judicial authorities, Union or Member State law could, (…), specify the processing operations and processing procedures in relation to the processing of personal data by 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 the judiciary in the performance of its judicial tasks. Supervision of such data processing operations may be entrusted to specific bodies within the judicial system of the Member State, which should in particular control compliance with the rules of this Regulation, promote the awareness of the judiciary of their obligations under this Regulation and deal with complaints in relation to such processing.

17) Directive 2000/31/EC does not apply to questions relating to information society services covered by this Regulation. That Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between Member States. Its application should not be affected by this Regulation. This Regulation should therefore be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

18) **(…)**[8]

……..

31) In order for processing to be lawful, personal data should be processed on the basis of the consent of the person concerned or some other legitimate legal basis laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. Whereas a legal basis does not necessarily require a legislative act adopted by a parliament[9], it 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**[10].

---

8 The text of this recital will be moved to a new recital 121a.

9 This sentence does not mandate Member States to adopt such rules in ways other than by acts of parliament, but merely allows them to do so.

10 Further to SI suggestion.

35a)This Regulation provides for general rules on data protection. However in specific cases Member States are also empowered to lay down national rules on data protection. The Regulation does therefore not exclude Member State law that defines the circumstances of specific processing situations, including determining more precisely the conditions under which processing of personal data is lawful. National law may also provide for special processing conditions for specific sectors and for the processing of special categories of data. National law may thus provide for *specific rules on the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective labour agreements, management, planning and organisation of work, equality and diversity in the workplace , health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship*.

36) Where processing is carried out in compliance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority, the processing should have a (…) basis in Union law or in the national law of a Member State. (…). It should be also for Union or national law to determine the purpose of the processing. Furthermore, this (…) basis could specify the general conditions of the Regulation[11] governing the lawfulness of data processing, determine specifications for determining the controller, the type of data which are subject to the processing, the data subjects concerned, the entities to which the data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing. It should also be for Union or national law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or by private law such as a professional association, where grounds of public interest so justify including for health purposes, such as public health and social protection and the management of health care services.

[11] DK would prefer to delete "of the Regulation" and refer simply to the general conditions.

37) The processing of personal data should equally be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's life or that of another person.

38) The legitimate interests of a controller including of a controller to which the data may be disclosed may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding. This would need careful assessment including whether a data subject can expect at the time and in the context of the collection of the data that processing for this purpose may take place. In particular such assessment must take into account whether the data subject is a child, given that children deserve specific protection. The data subject should have the right to object to the processing, on grounds relating to their particular situation and free of charge. To ensure transparency, the controller should be obliged to explicitly inform the data subject on the legitimate interests pursued and on the right to object, and also be obliged to document these legitimate interests. Given that it is for Union or national law to provide (…) the (…) basis for public authorities to process data, this legal ground should not apply for the processing by public authorities in the exercise of their public duties.

39) The processing of data to the extent strictly necessary for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems, by public authorities, Computer Emergency Response Teams – CERTs, Computer Security Incident Response Teams – CSIRTs, providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller *concerned*. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes can be regarded as carried out for a legitimate interest.[12]

[12] UK thought that this recital should also contain a reference to the use of pseudonymous data.

40) The processing of personal data for other purposes should be only allowed where the processing is compatible with those purposes for which the data have been initially collected, in particular where the processing is necessary for archiving **purposes in the public interest**, **or for** statistical, scientific or historical (…) purposes. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the data are initially collected, the controller should take into account any link between those purposes and the purposes of the intended further processing, the context in which the data have been collected, including the reasonable expectations of the data subject as to their further use, the nature of the personal data, the consequences of the intended further processing for data subjects, and appropriate safeguards. Where the intended other purpose is not compatible with the initial one for which the data are collected, the controller should obtain the consent of the data subject for this other purpose or should base the processing on another legitimate ground for lawful processing, in particular where provided by Union law or the law of the Member State to which the controller is subject. In any case, the application of the principles set out by this Regulation and in particular the information of the data subject on those other purposes should be ensured. Further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy.

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter and objectives

1. This Regulation lays down rules relating to the protection of individuals with regard to the processing of personal data and rules relating to the free movement of personal data[13].

2. This Regulation protects (…) fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

2a. **(…)** Member States may maintain or introduce national provisions to further specify the application of rules of this Regulation with regard to the processing of personal data **for compliance with a legal obligation or** for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or for other specific processing situations **as provided for in Article 6(1)(c) and (e)** by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing **including for other specific processing situations as provided for in Chapter IX**[14].

(…)

---

13 DE scrutiny reservation: DE thought that it was difficult to determine the applicability of EU data protection rules to the public sector according to internal market implications of the data processing operations.

14 This option was supported by PT, FR, IE, PL, LV, RO. Another option for a minimum harmonisation clause for the public sector (*Member States may maintain or introduce more stringent national provisions ensuring a higher level of protection of the rights and freedoms of the data subject, than those provided for in this Regulation, with regard to the processing of personal data by public authorities for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*) was supported by DK, NL, SE, SI and HR. ES could support both options. DE and HU expressed a preference for combining both options.

3. The free movement of personal data within the Union shall neither be restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.[15] [16].

Article 2

Material scope

1. This Regulation 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[17].

2. This Regulation does not apply to the processing of personal data:

   (a) in the course of an activity which falls outside the scope of Union law (…);

   (b) (…);

   (c) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V the Treaty on European Union;

   (d) by a natural person (…) in the course of (…) a personal or household activity;

---

[15] DK, FR, NL, SI scrutiny reservation. FR thought that this paragraph, which was copied from the 1995 Data Protection Directive (1995 Directive 95/46), did not make sense in the context of a Regulation as this was directly applicable.

[16] EE, FI, SE, and SI thought that the relation to other fundamental rights, such as the freedom of the press, or the right to information or access to public documents should be explicitly safeguarded by the operative part of the text of the Regulation. This is now regulated in Articles 80 and 80a of the draft Regulation.

[17] HU, supported by SI objected to the fact that data processing operations not covered by this phrase would be excluded from the scope of the Regulation and thought this was not compatible with the stated aim of a set of comprehensive EU data protection rules. HU therefore proposed to replace the second part by the following wording 'irrespective of the means by which personal data are processed'. COM argued that this was meant to exclude hand-written notes, but HU and SI thought that the means by which personal data were recorded should be immaterial.

(e) by competent public authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences and, for these purposes[18], safeguarding of public security[19], or the execution of criminal penalties.

3. (…).

CHAPTER II

PRINCIPLES

Article 6

Lawfulness of processing[20]

1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given unambiguous[21]consent to the processing of their personal data for one or more specific purposes[22];

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject (…)[23];

---

18 BE reservation on the terms 'for these purposes'.

19 The text needs to be aligned with the suggested text in the Data Protection Directive for police and judicial cooperation.

20 DE, AT, PT, SI, SE and SK scrutiny reservation.

21 FR, PL and COM reservation in relation to the deletion of 'explicit' in the definition of 'consent'; UK thought that the addition of 'unambiguous' was unjustified.

22 UK suggested reverting to the definition of consent in Article 2(h) of the 1995 Directive.

23 BG and ES scrutiny reservation; UK preferred the wording of the 1995 Directive.

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller[24] [25];

(f) processing is necessary for the purposes of the legitimate interests[26] pursued by the controller or by a controller to which the data are disclosed [27] except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This subparagraph shall not apply to processing carried out by public authorities in the exercise of their public duties[28] [29].

2. Processing of personal data which is necessary for **archiving purposes in the public interest**, **or for** historical, statistical or scientific **purposes** shall be **lawful** subject **also** to the conditions and safeguards referred to in Article 83[30].

3. The basis for the processing referred to in points (c) and (e) of paragraph 1 must be **established in accordance with**:

(a) Union law, or

(b) national law of the Member State to which the controller is subject.

---

[24] COM clarified that this was the main basis for data processing in the public sector. DE, DK, LT and UK asked what was meant by 'public interest' whether the application of this subparagraph was limited to the public sector or could also be relied upon by the private sector. FR also requested clarifications as to the reasons for departing from the text of the 1995 Directive. UK suggested reverting to the wording used in Article 7(e) of the 1995 Directive.

[25] Subparagraphs (d) and (e) might have to be inverted.

[26] FR scrutiny reservation.

[27] BG, CZ, DE, ES, HU, IT, NL, SE and UK asked to reinstate the words 'or by a third party' from the 1995 Directive. COM, supported by FR, thought that the use of the concept '*a* controller' should allow covering most cases of a third party.

[28] ES and FR scrutiny reservation. BE, DK, SI, PT and UK had suggested deleting the last sentence.

[29] DK and FR regretted there was no longer a reference to purposes set out in Article 9(2) and thought that the link between Article 6 and 9 needed to be clarified.

[30] Reinstated at the request of UK, FI and DE.

The purpose of the processing shall be determined in this legal basis or as regards the processing referred to in point (e) of paragraph 1, be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller[31]. This legal basis may **further** specify **the application of rules of this Regulation,** inter alia the general conditions governing the lawfulness of data processing the controller, the type of data which are subject to the processing, the data subjects concerned; the entities to, and the purposes for which the data may be disclosed; the purpose limitation[32]; storage periods and processing operations and processing procedures, including measures to ensure lawful and fair processing, **including for other specific processing situations as provided for in Chapter IX**.

3a. In order to ascertain whether a purpose of further processing is compatible with the one for which the data are initially collected, the controller shall take into account, inter alia[33]:

(a) any link between the purposes for which the data have been collected and the purposes of the intended further processing;

(b) the context in which the data have been collected;

(c) the nature of the personal data;

(d) the possible consequences of the intended further processing for data subjects;

(e) the existence of appropriate safeguards[34].

---

31 ES wanted start this sentence by stating: "While ensuring an equal or higher level of protection of the rights and freedoms of the data subject".

32 FR thought the purpose limitation might be further clarified in a recital.

33 DK, FI, NL, SI and SE stressed that the list should not be exhaustive. PT wanted to add consent by the data subject as an element.

34 BG, DE, ES and PL reservation: safeguards in themselves do not make further processing compatible.

4. Where the purpose of further processing is incompatible with the one for which the personal data have been collected, the <u>further</u> processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) [35] of paragraph 1 [36] [37] [38].

5. (…)

[35] FR and ES thought (f) should be added.

[36] DE, HU, IT, NL and PT scrutiny reservation. IT and PT thought paragraph 4 could be deleted.

[37] BE queried whether this allowed for a hidden 'opt-in', e.g. regarding direct marketing operations, which COM referred to in recital 40. BE, supported by FR, suggested adding 'if the process concerns the data mentioned in Articles 8 and 9'.

[38] HU thought that a duty for the data controller to inform the data subject of a change of legal basis should be added here: 'Where personal data relating to the data subject are processed under this provision the controller shall inform the data subject according to Article 14 before the time of or within a reasonable period after the commencement of the first operation or set of operations performed upon the personal data for the purpose of further processing not compatible with the one for which the personal data have been collected.'

CHAPTER III

SECTION 5

RESTRICTIONS

Article 21

Restrictions[39]

1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in **(…)**[40] Articles 12 to 20 and Article 32, when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard:

(aa) national security;

(ab) defence;

(a) public security;

---

[39] SI and UK scrutiny reservation. SE and UK wondered why paragraph 2 of Article 13 of the 1995 Data Protection Directive had not been copied here. DE, supported by DK, HU, RO, PT and SI, stated that para. 1 should not only permit restrictions of the rights of data subjects but also their extension. For example, Article 20(2)(b) requires that Member States lay down 'suitable measures to safeguard the data subject's legitimate interests', which, when they take on the form of extended rights of access to information as provided for under German law in the case of profiling to asses creditworthiness (credit scoring), go beyond the Proposal for a Regulation. With an eye to Article 6(3), the Member States also need flexibility especially in the public sector or in the health sector when it comes to laying down and framing specific rules (esp. in regard to earmarking, the nature of the data and the recipient) and enacting stricter rules. DE and EE thought the derogations should distinguish between the private and the public sector.

[40] Further to the remarks by BE, DE, HU, FI, FR, LU, AT and PL the reference to Article 5 has been deleted, as the principles of Article 5 should never be derogated from. IE and UK opposed this; with IE citing the example of 'unfair' data collection by insurance companies which might be necessary to rebut false damage claims.

(b) the prevention, investigation, detection and prosecution of criminal offences and, for these purposes, safeguarding public security[41], or the execution of criminal penalties;

(c) other important objectives of general public interests of the Union or of a Member State[42], in particular an important[43] economic or financial interest of the Union or of a Member State, including, monetary, budgetary and taxation matters**, public health and social security**[44]**,** the protection of market stability and integrity

(ca) the protection of judicial independence and judicial proceedings;

(d) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(e) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in **(aa), (ab),** (a), (b), (c) and (d);

(f) the protection of the data subject or the rights and freedoms of others;

(g) **the enforcement of civil law claims**[45].

---

41 This change in wording will need to be discussed, but the Presidency has suggested this change in order to align the text to the suggested text in the Data Protection Directive for police and judicial cooperation.

42 DE, IT scrutiny reservation as to the broad character of this exemption. SE thought it should be moved to a separate subparagraph.

43 DK, FR and UK scrutiny reservation on the adjective 'important'.

44 BE and FR suggestion.

45 Further to DE proposal.

2. Any legislative measure referred to in paragraph 1 shall contain specific provisions at least as to the purposes of the processing or categories of processing, the categories of personal data, the scope of the restrictions introduced, the specification of the controller or categories of controllers, **the storage period** and the applicable safeguards taking into account of the nature, scope and purposes of the processing and the risks for the rights and freedoms of data subjects.