Analysis

The Proposed Data Protection Regulation:

What has the Council agreed so far?

Steve Peers, Professor of Law, University of Essex
Twitter: @StevePeers

8 December 2014

Introduction

Back in January 2012, the Commission proposed a new data protection Regulation that would replace the EU's existing Directive on the subject. It also proposed a new Directive on data protection in the sphere of law enforcement, which would replace the current 'Framework Decision' on that subject.

Nearly three years later, there has been some gradual progress on discussing these proposals. The European Parliament (which has joint decision-making power on both proposals) adopted its positions back in the spring. For its part, the EU Council (which consists of Member States' justice ministers) has been adopting its position on the proposed Regulation in several pieces. It has not yet adopted even part of its position on the proposed Directive.

For the benefit of those interested in the details of these developments, the following analysis presents a consolidated text of the three pieces of the proposed Regulation which the Council has agreed to date, including the parts of the preamble which have already been agreed. I have left intact the footnotes appearing in the agreed texts, which set out Member States' comments.

The underline, italics and bold text indicate changes from the Commission proposal. I have added a short summary of the subject-matter of the Chapters and Articles in the main text which have not yet been agreed by the Council.

For detailed analyses of some parts of the texts agreed so far, see the links to the two blog posts.

The Council might always change its current position at a later point, and of course the final text of the new legislation will also depend on negotiations between the Council and the European Parliament.

Background documents

'Public sector' provisions, agreed by Dec. 2014 JHA Council:

http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2016140%202014%20INIT

Chapter IV, agreed by Oct. 2014 JHA Council:

http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2013772%202014%20INIT

Rules on territorial scope, agreed by June 2014 JHA Council:

http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010349%202014%20INIT

Proposal from Commission:

http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

Position of European Parliament:

http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%207427%202014%20REV%201

Analysis of agreed territorial scope rules:

http://eulawanalysis.blogspot.co.uk/2014/06/reforming-eu-data-protection-law.html

Analysis of agreed 'privacy seals' rules:

http://eulawanalysis.blogspot.co.uk/2014/10/warning-eu-council-is-trying-to.html

'The Proposed Data Protection Regulation, as agreed to date by the Council'.

Preamble

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 for compliance with a legal obligation,[1] 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. In conjunction with the general and horizontal law on data protection implementing Directive 95/46/EC Member States have several sector specific laws in areas that need more specific provisions. This Regulation also provides a margin of manoeuvre for Member States to specify its rules. Within this margin of manoeuvre sector-specific laws that Member States have issued

[1] AT, supported by SI, made a proposal for a separate Article 82b which would allow Member States to adopt specific private sector provisions for specific situations (15768/14 DATAPROTECT 176 JAI 908 MI 916 DRS 156 DAPIX 179 FREMP 215 COMIX 623 CODEC 2300). The Presidency thinks that the revised recital 8 read together with Article 1(2a) sufficiently caters for this concern.

implementing Directive 95/46/EC should be able to be upheld.

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 (…), 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. (…)

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. (…).

19) Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union or not. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in this respect.

20) In order to ensure that individuals are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects residing in the Union by a controller not established in the Union should be subject to this Regulation where the processing activities are related to the offering of goods or services to such data subjects irrespective of whether connected to a payment or not, which takes place in the Union. In order to determine whether such a controller is offering goods or services to such data subjects in the Union, it should be ascertained whether it is apparent that the controller is envisaging doing business with data subjects residing in one or more Member States in the Union. Whereas the mere accessibility of the controller's or an intermediary's website in the Union or of an email address and of other contact details or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, and/or the mentioning of customers or users residing in the Union, may make it apparent that the controller envisages offering goods or services to such data subjects in the Union.

21) The processing of personal data of data subjects residing in the Union by a controller not established in the Union should also be subject to this Regulation when it is related to the monitoring of their behaviour taking place within the European Union. In order to determine whether a processing activity can be considered to 'monitor the

behaviour' of data subjects, it should be ascertained whether individuals are tracked on the internet with data processing techniques which consist of profiling an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.

22) Where the national law of a Member State applies by virtue of public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State's diplomatic mission or consular post.

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.

31a) Wherever this Regulation 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.

35a) This Regulation provides for general rules on data protection **and that** 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.

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 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.

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.

59) Restrictions on specific principles and on the rights of information, access, rectification and erasure or on the right to data portability, the right to object, measures based on profiling, as well as on the communication of a personal data breach to a data subject

and on certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or man made disasters, the prevention, investigation and prosecution of criminal offences or of breaches of ethics for regulated professions, other public interests of the Union or of a Member State in particular an important economic or financial interest of the Union or of a Member State, the keeping of public registers **kept for reasons of general public interest**, further processing of archived personal data to provide specific information related to the political behaviour under former totalitarian state regimes or the protection of the data subject or the rights and freedoms of others, including social protection and public health. Those restrictions should be in compliance with requirements set out by the Charter of Fundamental Rights of the European Union and by the European Convention for the Protection of Human Rights and Fundamental Freedoms.

60) 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 this Regulation (…). These measures should take into account the nature, scope, context and purposes of the processing and the risk for the rights and freedoms of individuals.

60a) Such risks, 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, [breach of (…) pseudonymity][2], 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 evaluated, in particular analysing and prediction of aspects concerning performance at work, economic situation, health, personal preferences or interests,

[2] The reference to the use of pseudonymous data in Chapter IV will in the future need to be debated in the context of a further debate on pseudonymising personal data.

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; (…).

60b) *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*[3] *risk of prejudice to the rights and freedoms of individuals* (…).

60c) Guidance for the implementation of appropriate measures, and for demonstrating the compliance by the controller [or processor], especially as regards the identification of the risk related to the processing, their assessment in terms of their origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk, could be provided in particular by approved codes of conduct, approved certifications, guidelines of the European Data Protection Board or through the indications provided by a data protection officer. The European Data Protection Board may also issue guidelines on processing operations that are considered to be unlikely to result in a high risk for the rights and freedoms of individuals and indicate what measures may be sufficient in such cases to address such risk. (…)

61) The protection of the rights and freedoms of individuals with regard to the processing of personal data require that appropriate technical and organisational measures are taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default. Such measures could consist inter alia of minimising the processing of personal data, (…) pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that

[3] The use the word 'particular' was questioned by BE, CZ, ES and UK, which thought that this term does not express the seriousness of the risk in case of 'high' risk.

are either based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.

62) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processor**s**, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities under this Regulation, including where a controller determines the purposes (…) and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

63) Where a controller not established in the Union is processing personal data of data subjects residing in the Union whose processing activities are related to the offering of goods or services to such data subjects, or to the monitoring of their behaviour in the Union, (…) the controller should designate a representative, unless (…) *the processing it carries out is* **occasional and unlikely** *to result in a risk for the rights and freedoms of data subjects, taking into account the nature, scope, context and purposes of the processing* **or** the controller is a public authority or body (…). The representative should act on behalf of the controller and may be addressed by any supervisory authority. The representative should be explicitly designated by a written mandate of the controller to act on its behalf with regard to the latter's obligations under this Regulation. The designation of such representative does not affect the responsibility and liability of the controller under this Regulation. Such representative should perform its tasks according to the received mandate from the controller, including to cooperate with the competent supervisory authorities on any action taken in ensuring compliance with this Regulation. The designated representative should be subjected to enforcement actions in case of non-compliance by the controller.

63a) To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge,

reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing. (…) Adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller. The carrying out of processing by a processor should be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purpose**s** of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk for the rights and freedoms of the data subject.

The controller and processor may choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by a supervisory authority in accordance with the consistency mechanism and then adopted by the Commission, or which are part of a certification granted in the certification mechanism. After the completion of the processing on behalf of the controller, the processor should return or delete the personal data, unless there is a requirement to store the data under Union or Member State law to which the processor is subject.

64) (…)

65) In order to demonstrate compliance with this Regulation, the controller or processor should maintain records regarding all categories of processing activities under its responsibility. 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 those processing operations.

66) In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should evaluate the (…) risks inherent to the processing and implement measures to mitigate those risk. These measures should ensure an appropriate level of security, including confidentiality, taking into account available technology and the costs of (…) implementation in relation to the risk and the nature of the personal data to be protected. (…). In assessing data security risk, consideration should be given to the risk**s** that are presented by data processing,

such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed, which may in particular lead to physical, material or moral damage.

66a) In order to enhance compliance with this Regulation in cases where the processing operations are likely to result in a high risk for the rights and freedoms of individuals, the controller [or the processor] should be responsible for the carrying out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of this risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data is in compliance with this Regulation. Where a data protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.

67) 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, [breach of (…) pseudonymity], damage to the reputation, loss of confidentiality of data protected by professional secrecy or any other economic or social disadvantage to the individual concerned. (…). Therefore, as soon as the controller becomes aware that (…) a personal data breach which may result in (…) physical, material or moral damage has occurred the controller should notify the breach to the supervisory authority without undue delay and, where feasible, within 72 hours. Where this cannot be achieved within 72 hours, an explanation of the reasons for the delay should accompany the notification. The individuals whose rights and freedoms could be severely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. (…). The notification should describe the nature of the personal data breach as well as recommendations for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities). For example (…) the need to mitigate an immediate risk of damage would call for a prompt notification of

data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay.

68) **(…)** It must be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject (…). The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation.

68a) 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 the personal data (…).

69) 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 identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law enforcement authorities in cases where early disclosure could unnecessarily hamper the investigation of the circumstances of a breach.

70) Directive 95/46/EC provided for a general obligation to notify processing of personal data to the supervisory authorities. While this obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Therefore such indiscriminate general notification obligations should be abolished, and replaced by effective procedures and mechanisms which focus instead on those types of processing operations which are likely to result in a high risk to the rights and freedoms of individuals by virtue of their nature, scope, *context*

and purposes (…). Such types of processing operations may be those which, in particular, involve using new technologies, or are of a new kind and where no data protection impact assessment has been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing[4].

70a) In such cases, a data protection impact assessment should be carried out by the controller (…) prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, *context and* purposes of the processing and the sources of the risk, which should include in particular the envisaged measures, safeguards and mechanisms for mitigating that risk and for ensuring the protection of personal data and for demonstrating the compliance with this Regulation.

71) This should in particular apply to (…) large-scale processing operations, which aim at processing a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk, for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high (…) risk for the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights. A data protection impact assessment should also be made in cases where data are processed for taking decisions regarding specific individuals following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures. A data protection impact assessment is equally required for monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices or for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk for the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale. *The processing of (…) personal data irrespective of*

[4] BE was opposed to the temporal reference in the last part of this sentence.

the volume or the nature of the data, should not be considered as being on a large scale, if the processing of these data is protected by professional secrecy (…), such as the processing of personal data from patients or clients by an individual doctor, health care professional, hospital or attorney. In these cases a data protection impact assessment should not be mandatory.

72) There are circumstances under which it may be sensible and economic that the subject of a data protection impact assessment should be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.

73) Data protection impact assessments may be carried out by a public authority or public body if such an assessment has not already been made in the context of the adoption of the national law on which the performance of the tasks of the public authority or public body is based and which regulates the specific processing operation or set of operations in question.

74) Where a data protection impact assessment indicates that the processing would, despite the envisaged safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of individuals (…), and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the supervisory authority should be consulted, prior to the start of the processing activities. Such high (…) risk is likely to result from certain types of data processing and certain extent and frequency of processing, which may result also in a realisation of (…) damage or (…) interference with the rights and freedoms of the data subject. The supervisory authority should respond to the request for consultation in a defined period. However, the absence of a reaction of the supervisory authority within this period should be without prejudice to any intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation, including the power to prohibit processing operations. As part of this consultation process, the outcome of a data protection impact assessment carried out with regard to the processing at issue

pursuant to Article 33 may be submitted to the supervisory authority, in particular the measures envisaged to mitigate the risk for the rights and freedoms of individuals.

74a) The processor should assist the controller, where necessary and upon request, in ensuring compliance with the obligations deriving from the carrying out of data protection impact assessments and from prior consultation of the supervisory authority.

74b) A consultation with the supervisory authority should also take place in the course of the preparation of a legislative or regulatory measure which provides for the processing of personal data (…), in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risk involved for the data subject.

75) Where the processing is carried out in the public sector or where, in the private sector, processing is carried out by a large enterprise, or where its core activities, regardless of the size of the enterprise, involve processing operations which require regular and systematic monitoring, a person with expert knowledge of data protection law and practices may assist the controller or processor to monitor internal compliance with this Regulation. Such data protection officers, whether or not an employee of the controller, should be in a position to perform their duties and tasks in an independent manner.

76) Associations or other bodies representing categories of controllers or processors should be encouraged to draw up codes of conduct, within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors and the specific needs of micro, small and medium enterprises. In particular such codes of conduct could calibrate the obligations of controllers and processors, taking into account the risk likely to result from the processing for the rights and freedoms of individuals.

76a) When drawing up a code of conduct, or when amending or extending such a code, associations and other bodies representing categories of controllers or processors should consult with relevant stakeholders, including data subjects where feasible,

and have regard to submissions received and views expressed in response to such consultations.

77) In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms, data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services.

78) Cross-border flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international co-operation. The increase in these flows has raised new challenges and concerns with respect to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of individuals guaranteed in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or[5] another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer may only take place if, subject to the other provisions of this Regulation, the conditions laid down in Chapter V are complied with by the controller or processor.

79) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects. Member States may conclude international agreements which involve the transfer of personal data to third countries or international organisations, as far as such agreements do not affect this Regulation or any other provisions of EU law and include safeguards to protect the rights of the data subjects[6].

[5] DE scrutiny reservation, querying especially about the application of the rules of place of purchase in relation to Article 89a.

[6] FR requests the second sentence to be inserted in Article 89a. NL asked what was meant with the new text and considered that it was necessary to keep it, but its purpose and meaning should be clarified. DE and UK scrutiny reservation on the new text. EE asked whether if "*affect*" means that it was not contradictory or something else.

80) The Commission may (…) decide with effect for the entire Union that certain third countries, or a territory or a specified sector, such as the private sector or one or more specific economic 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.

81) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of a third country or of a territory or of a specified sector within a third country, 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. The adoption of an adequacy decision to a territory or a specified sector in a third country should take into account clear and objective criteria , such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country.

81a) Apart from the international commitments the third country or international organisation has entered into, the Commission should also take account of obligations arising from the third country's or international organisation's participation in multilateral or regional systems in particular in relation to the protection of personal data, as well as the implementation of such obligations. In particular the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol *should be taken into account*. The Commission should consult with the European Data Protection Board when assessing the level of protection in third countries or international organisations[7].

[7] DE, supported by NL, proposed that the list of checks in Article 42(2) should include a new component consisting of the participation of third states or international organisations in international data-protection systems (e.g. APEC and ECOWAS). According to the position of DE, although those systems are still in the early stages of practical implementation, the draft Regulation should make allowance right away for the significance they may gain in future. Point (d) of Article 41(2) requires the systems to be fundamentally suited to ensuring compliance with data protection standards.

81b) The Commission should monitor the functioning of decisions on the level of protection in a third country or a territory or specified sector within a third country, or an international organisation, including decisions adopted on the basis of Article 25(6) or Article 26 (4) of Directive 95/46/EC. The Commission should evaluate, within a reasonable time, the functioning of the latter decisions and report any pertinent findings to the Committee within the meaning of Regulation (EU) No 182/2011 as established under this Regulation.

82) The Commission may (…) 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 42 to 44 are fulfilled. In that case, provision should be made 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.

83) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or ad hoc contractual clauses authorised by a supervisory authority, or other suitable and proportionate measures justified in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations and where authorised by a supervisory authority. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects, including the right to obtain effective administrative or judicial redress. They should relate in particular to compliance with the general principles relating to personal data processing, the availability of enforceable data subject's rights and of effective legal remedies and the principles of data protection by design and by default. Transfers may be carried out also by public authorities or bodies with public authorities or bodies in third countries or with international organisations with corresponding duties or functions, including on the basis of provisions to be inserted into administrative arrangements, such as a memorandum of understanding. The authorisation of the competent supervisory authority should be obtained when the safeguards are adduced in non legally binding administrative arrangements.

84) The possibility for the controller or processor to use standard data protection clauses adopted by the Commission or by a supervisory authority should neither prevent the possibility for controllers or processors to include the standard data protection clauses in a wider contract, including in a contract between the processor and another processor, nor to add other clauses or additional safeguards as long as they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects.

85) A corporate group or a group of enterprises engaged in a joint economic activity should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same corporate group of undertakings or group of enterprises, as long as such corporate rules include essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.

86) Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his explicit consent, where the transfer is occasional **(...)** in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies. Provision should also be made for the possibility for transfers where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In this latter case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients.

87) These rules should in particular apply to data transfers required and necessary for important reasons of public interest, for example in cases of international data exchange, between competition authorities, between tax or customs administrations, between financial supervisory authorities, between services competent for social security matters or for public health, for example in case of contact tracing for contagious diseases or in order to reduce and/or eliminate doping in sport. A transfer 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 or another person's vital interests,

including physical integrity or life, if the data subject is incapable of giving consent.[8] In the absence of an adequacy decision, Union law or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of data to a third country or an international organization. Member States should notify such provisions to the Commission.

88) Transfers which cannot be qualified as large scale or frequent, could also be possible for the purposes of the legitimate interests pursued by the controller or the processor, when those interests are not overridden by the interests or rights and freedoms of the data subject and when the controller or the processor has assessed all the circumstances surrounding the data transfer. The controller or processor should give particular consideration to the nature of the data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and adduced suitable safeguards to protect fundamental rights and freedoms of natural persons with respect to processing of their personal data. For the purposes of processing for historical, statistical and scientific research purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration. To assess whether a transfer is large scale or frequent the amount of personal data and number of data subjects should be taken into account and whether the transfer takes place on an occasional or regular basis.

89) In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with a guarantee that they will continue to benefit from the fundamental rights and safeguards as regards processing of their data in the Union once this data has been transferred.

90) Some third countries enact laws, regulations and other legislative instruments which purport to directly regulate data processing activities of natural and legal persons under the jurisdiction of the Member States. The extraterritorial application of these laws, regulations and other legislative instruments may be in breach of international law and may impede the attainment of the protection of individuals guaranteed in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may inter alia be the case

[8] FR referred to the situation of a recipient of the transfer who is a medical professional or has adduced provisions ensuring the respect of the data subject's right to privacy and medical confidentiality. PRES considers that this could be further addressed in the context of chapter IX.

where the disclosure is necessary for an important ground of public interest recognised in Union law or in a Member State law to which the controller is subject. (…)

91) When personal data moves across borders outside the Union it may put at increased risk the ability of individuals to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities 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 preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, there is a need to promote closer co-operation among data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts. For the purposes of developing international co-operation mechanisms to facilitate and provide international mutual assistance for the enforcement of legislation for the protection of personal data, the Commission and the supervisory authorities should exchange information and cooperate in activities related to the exercise of their powers with competent authorities in third countries, based on reciprocity and in compliance with the provisions of this Regulation, including those laid down in Chapter V.

107) At Union level, a European Data Protection Board should be set up. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of a head of a supervisory authority of each Member State and of the European Data Protection Supervisor. The Commission should participate in its activities without voting rights. The European Data Protection Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission, in particular on the level of protection in third countries or international organisations, and promoting co-operation of the supervisory authorities throughout the Union. The European Data Protection Board should act independently when exercising its tasks.

121) Member States law should reconcile the rules governing freedom of expression and information, including journalistic, academic, artistic and or literary expression with the right to the protection of personal data pursuant to this Regulation. The processing of personal data for journalistic purposes, or for the purposes of

academic, artistic or literary expression should be subject to derogations or exemptions from certain provisions of this Regulation if necessary to reconcile the right to the protection of personal data, with the right to freedom of expression and information, as guaranteed by Article 11 of the Charter of Fundamental Rights of the European Union. This should apply in particular to processing of personal data in the audiovisual field and in news archives and press libraries. Therefore, Member States should adopt legislative measures, which should lay down exemptions and derogations which are necessary for the purpose of balancing these fundamental rights. Such exemptions and derogations should be adopted by the Member States on general principles, on the rights of the data subject, on controller and processor, on the transfer of data to third countries or international organisations, on the independent supervisory authorities, on co-operation and consistency. In case these exemptions or derogations differ from one Member State to another, the national law of the Member State to which the controller is subject should apply. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly. (…)

121a) *This Regulation allows the principle of public access to official documents to be taken into account when applying the provisions set out in this Regulation. Public access to official documents may be considered as a public interest. Personal data in documents held by a public authority or a public body should be able to be publicly disclosed by this authority or body if the disclosure is provided for by Union law or Member State law to which the public authority or public body is subject. Such laws should reconcile public access to official documents and the reuse of public sector information with the right to the protection of personal data and may therefore provide for the necessary derogations from the rules of this regulation. The reference to public authorities and bodies should in this context include all authorities or other bodies covered by Member State law on public access to documents. Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information leaves intact and in no way affects the level of protection of individuals with regard to the processing of personal data under the provisions of Union and national law, and in particular does not alter the obligations and rights set out in this Regulation. In particular, that Directive should not apply to documents access to which is excluded or restricted by virtue of the access regimes*

on the grounds of protection of personal data, and parts of documents accessible by virtue of those regimes which contain personal data the re-use of which has been defined by law as being incompatible with the law concerning the protection of individuals with regard to the processing of personal data[9].

122) (…)[10].

123) (…)[11].

124) National law or collective agreements **(including 'works agreements')**[12] may 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 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*.

125) The processing of personal data for historical, statistical or scientific (…) purposes and for archiving purposes (…) should, in addition to the general principles and specific rules of this Regulation, in particular as regards the conditions for lawful processing, also comply with respect other relevant legislation such as on clinical trials. The further processing of personal data for historical, statistical and scientific purposes and for archiving purposes (…) should not be considered incompatible with the purposes for which the data are initially collected and may be processed for those purposes for a longer period than necessary for that initial purpose (…). Member States should be authorised to provide, under specific conditions and in the presence of appropriate safeguards for data subjects, specifications and derogations to the information requirements and the rights to access, rectification, erasure, to be forgotten, restriction of processing and on the right to data portability and the right to object when processing personal data for historical, statistical or scientific purposes and for archiving purposes (…) The conditions and safeguards in question may entail specific procedures for data subjects to exercise those rights if this is appropriate in

---

9 Moved from recital 18.
10 Moved to recital 42a.
11 Moved to recital 42b.
12 DE proposal.

the light of the purposes sought by the specific processing along with technical and organisational measures aimed at minimising the processing of personal data in pursuance of the proportionality and necessity principles.

125a) (…)[13].

125aa) By coupling information from registries, researchers can obtain new knowledge of great value when it comes to e.g. widespread diseases as cardiovascular disease, cancer, depression etc. On the basis of registries, research results can be enhanced, as they draw on a larger population. Within social science, research on the basis of registries enables researchers to obtain essential knowledge about long-term impact of a number of social conditions e.g. unemployment, education, and the coupling of this information to other life conditions. Research results obtained on the basis of registries provide solid, high quality knowledge, which can provide the basis for the formulation and implementation of knowledge-based policy, improve the quality of life for a number of people, and improve the efficiency of social services etc.
In order to facilitate scientific research, personal data can be processed for scientific purposes subject to appropriate conditions and safeguards set out in Member State or Union law. Hence consent from the data subject should not be necessary for each further processing for scientific **purposes**.

125b) The importance of archives for the understanding of the history and culture of Europe" and "that well-kept and accessible archives contribute to the democratic function of our societies', were underlined by Council Resolution of 6 May 2003 on archives in the Member States[14]. Where personal data are processed for archiving purposes, this Regulation should also apply to that processing, bearing in mind that this Regulation should not apply to deceased persons.

Public authorities or public or private bodies that hold records of public interest should be services which, pursuant to Union or Member State law, have a legal obligation to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest. Member States should also be authorised to provide that personal data may

[13] Moved to recitals 126c and 126d.
[14] OJ C 113, 13.5.2003, p. 2.

be further processed for archiving purposes, for example with a view to providing specific information related to the political behaviour under former totalitarian state regimes[15].

Codes of conduct may contribute to the proper application of this Regulation, including when personal data are processed for archiving purposes in the public interest by further specifying appropriate safeguards for the rights and freedoms of the data subject[16]. Such codes should be drafted by Member States' official archives or by the European Archives Group. Regarding international transfers of personal data included in archives, these must take place without prejudice of the applying European and national rules for the circulation of cultural goods and national treasures.

126) Where personal data are processed for scientific purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, processing of personal data for scientific purposes should include fundamental research, applied research, privately funded research[17] and in addition should take into account the Union's objective under Article 179(1) of the Treaty on the Functioning of the European Union of achieving a European Research Area. Scientific purposes should also include studies conducted in the public interest in the area of public health. To meet the specificities of processing personal data for scientific purposes specific conditions should apply in particular as regards the publication or otherwise disclosure of personal data in the context of scientific purposes. If the result of scientific research in particular in the health context gives reason for further measures in the interest of the data subject, the general rules of this Regulation should apply in view of those measures[18].

126a) Where personal data are processed for historical purposes, this Regulation should also apply to that processing. This should also include historical research and research for genealogical purposes, bearing in mind that this Regulation should not apply to deceased persons..

126b) For the purpose of consenting to the participation in scientific research activities in clinical trials (…) the relevant provisions of Regulation (EU) No. 536/2014 of the

15 CZ reservation.
16 CZ, DK, FI, HU, FR, MT, NL, PT, RO, SE, SI and UK scrutiny reservation.
17 AT and SE scrutiny reservation.
18 CZ, DK, FI, FR, HU, MT, NL, PT, SE, SI and UK scrutiny reservation.

European Parliament and of the Council should apply.

126c) Where personal data are processed for statistical purposes, this Regulation should apply to that processing. *Union law or Member State law should, within the limits of this Regulation, determine statistical content, control of access, specifications for the processing of personal data for statistical purposes and appropriate measures to safeguard the rights and freedoms of the data subject and for guaranteeing statistical confidentiality.*

126d) *The confidential information which the Union and national statistical authorities collect for the production of official European and official national statistics should be protected. European statistics should be developed, produced and disseminated in conformity with the statistical principles as set out in Article 338(2) of the Treaty of the Functioning of the European Union, while national statistics should also comply with national law.*

Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities[19] provides further specifications on statistical confidentiality for European statistics.

127) As regards the powers of the supervisory authorities to obtain from the controller or processor access personal data and access to its premises, Member States may adopt by law, within the limits of this Regulation, specific rules in order to safeguard the professional or other equivalent secrecy obligations, in so far as necessary to reconcile the right to the protection of personal data with an obligation of professional secrecy. This is without prejudice to existing Member State obligations to adopt professional secrecy where required by Union law.

128) This Regulation respects and does not prejudice the status under **existing constitutional** law of churches and religious associations or communities in the

[19] OJ L 87, 31.3.2009, p. 164–173.

Member States, as recognised in Article 17 of the Treaty on the Functioning of the European Union. (...).

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.

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 more specific provisions to adapt the application of the 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[20].

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[21].

[NOT YET AGREED: Article 2: Material scope]

[20] AT, CZ, HU, SI and SK reservation; these delegations were in favour of a minimum harmonisation clause for the public sector. LU reservation: this offers too much leeway.

[21] DK, FR, NL, SI scrutiny reservation.

Article 3

Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.

2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:

   (a) the offering of goods or services, irrespective of whether a payment by the data subject is required, to such data subjects in the Union; or

   (b) the monitoring of their behaviour as far as their behaviour takes place within the European Union[22].

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.

Article 4

Definitions

For the purposes of this Regulation:

(17) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State of the Union for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings[23] or group of enterprises engaged in a joint economic activity;

[22] UK reservation.

[23] DE queried whether BCRs could also cover intra-EU data transfers. COM indicated that there was no need for BCRs in the case of intra-EU transfers, but that controllers were free to apply BCRs also in those cases.

(21) 'international organisation' means an organisation and its subordinate bodies governed by public international law or any other body which is set up by, or on the basis of, an agreement between two or more countries[24];

[NOT YET AGREED: other definitions in Article 4]

CHAPTER II

PRINCIPLES

[NOT YET AGREED: Article 5: Principles of data protection]

Article 6

Lawfulness of processing[25]

[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[26]consent to the processing of their personal data for one or more specific purposes[27];

(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 (…)[28];

(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;

(f) processing is necessary for the purposes of the legitimate interests[29] pursued by the controller or by a third party [30] except where such interests are overridden by the interests or fundamental rights and freedoms of the data

---

24 NL queried whether MOUs would also be covered by this definition; FI queried whether Interpol would be covered. CZ, DK, LV, SI, SE and UK pleaded in favour of its deletion.

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

26 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.

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

28 BG scrutiny reservation; UK preferred the wording of the 1995 Directive.

29 FR scrutiny reservation.

30 Reinstated at the request of BG, CZ, DE, ES, HU, IT, NL, SE, SK and UK.

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[31] [32]].

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.

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.

   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. This legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia the general conditions governing the lawfulness of data processing **by** 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; 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;

---

31 BE, DK, MT SI, PT and UK had suggested deleting the last sentence. FR scrutiny reservation.

32 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.

33 DK, FI, NL, SI and SE stressed the list should not be exhaustive. PT: add consent.

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

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

4. Where the purpose of further processing is incompatible with the one for which the personal data have been collected, the further 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. (…)

[NOT YET AGREED: the rest of Chapter II:

including consent, children, sensitive data]

CHAPTER III

[NOT YET AGREED: Sections 1 to 4 of Chapter III (rights of the data subject),

including right of access, right to be forgotten]

SECTION 5
RESTRICTIONS

[34] BG, DE and PL reservation: safeguards as such do not make further processing compatible.

[35] DK, DE, ES FR and NL thought (f) should be added.

[36] DE, HU, NL and PT scrutiny reservation. 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.'

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 (…) Articles 12 to 20 and Article 32, as well as Article 5[40] in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 20, 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.

[40] AT reservation.

(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, in particular an important economic or financial interest of the Union or of a Member State, including, monetary, budgetary and taxation matters, public health and social security, 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.

2. Any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, 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 periods and the applicable safeguards taking into account of the nature, scope and purposes of the processing or categories of processing and the risks for the rights and freedoms of data subjects.

[41] The wording of points (b), and possibly also point (a), will have to be discussed again in the future in the light of the discussions on the relevant wording of the text of the Data Protection Directive for police and judicial cooperation.

CHAPTER IV

CONTROLLER AND PROCESSOR[42]

SECTION 1

GENERAL OBLIGATIONS

Article 22

Obligations of the controller

1. 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 shall (…) implement appropriate measures and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.

2. (…)

2a. Where proportionate in relation to the processing activities[43], the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

2b. Adherence to approved codes of conduct pursuant to Article 38 or an approved certification mechanism pursuant to Article 39 may be used as an element to demonstrate compliance with the obligations of the controller.

3. (…)

4. (…)

[42] SI and UK scrutiny reservation on the entire chapter. BE, DE, NL and UK have not been not convinced by the figures provided by COM according to which the reduction of administrative burdens doing away with the general notification obligation on controllers, outbalanced any additional administrative burdens and compliance costs flowing from the proposed Regulation.

[43] HU, RO and PL thought this wording allowed too much leeway to controllers. AT thought that in particular for the respects to time limits and the reference to the proportionality was problematic.

Article 23

Data protection by design and by default

1. (…) Having regard to available technology and the cost of implementation and taking account of *the nature, scope, context and purpose**s** of the processing* as well as the likelihood and severity of the risk for rights and freedoms of individuals posed by the processing, the controllers shall implement (…) technical and organisational measures appropriate to the processing activity being carried out and its objectives, [including minimisation and pseudonymisation[44]], in such a way that the processing will meet the requirements of this Regulation and protect the rights of (…) data subjects.

2. The controller shall implement appropriate measures for ensuring that, by default, only (…) personal data (…) which are necessary[45] 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. Where the purpose of the processing is not intended to provide the public with information, those mechanisms shall ensure that by default personal data are not made accessible without human intervention to an indefinite number of individuals.

2a. An approved certification mechanism pursuant to Article 39 *may be used as an element* to demonstrate compliance with the requirements set out in paragraphs 1 and 2.

3. (…)

4. (…)

[44] DE thought that, in view of Article 5(c), the principle of data economy and avoidance, as well as anonymisation and pseudonymisation should be listed as key options for implementation. This debate will however need to take place in the context of a debate on pseudonymising personal data.

[45] CZ would prefer "not excessive". This term may be changed again in the future in the context of the debate on the wording of Article 5(1)(c).

Article 24

Joint controllers[46]

1. 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 obligations under this Regulation, in particular as regards the (…) exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 14 and 14a, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement shall designate which of the joint controllers shall act as single point of contact for data subjects to exercise their rights.

2. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the (…) controllers.

3. The arrangement shall duly reflect the joint controllers' respective effective roles and relationships vis-à-vis data subjects, and the essence of the arrangement shall be made available for the data subject. Paragraph 2 does not apply where the data subject has been informed in a transparent and unequivocal manner which of the joint controllers is responsible, unless such arrangement other than one determined by Union or Member State law is unfair with regard to his or her rights (…).

[46] SI reservation; it warned against potential legal conflicts on the allocation of the liability and SI therefore thought this article should be further revisited in the context of the future debate on Chapter VIII. FR also thought the allocation of liability between the controller and the processor is very vague and CZ expressed doubts about the enforceability of this provision in the private sector outside arrangements within a group of undertakings and thought it should contain a safeguard against outsourcing of responsibility.

Article 25

Representatives of controllers not established in the Union

1. Where Article 3(2) applies, the controller shall designate in writing a representative in the Union.

2. This obligation shall not apply to:

   (a) (…); or

   (b) *processing which is* **occasional**[47] **and** *unlikely to result in a* (…) *risk for the rights and freedoms of individuals, taking into account the nature, context, scope and purposes of the processing* (…); or

   (c) a public authority or body;

   (d) (…)

3. The representative shall be established in one of those Member States where the data subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, reside.

3a. The representative shall be mandated by the controller to be addressed in addition to or instead of the controller by, in particular, supervisory authorities and data subjects, on all issues related to the processing of personal data, for the purposes of ensuring compliance with this Regulation.

4. The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself.

[47] HU, SE and UK reservation.

Article 26

Processor

1. (…).[48] 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 this Regulation (…).

1a. 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[49].

1b. (…)[50].

2. The carrying out of processing by a processor shall be governed by a contract or **a** legal act under Union or Member State law binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and 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:

   (a) process the personal data only on instructions from the controller (…), unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing the data, unless that law prohibits such information on important grounds of public interest;

---

48 The Presidency suggest completing Article 5(2) with the words "also in case of personal data being processed on its behalf by a processor". This may also need further discussion in the context of the future debate on liability in the context of Chapter VIII.

49 LU and FI were concerned that this might constitute an undue interference with contractual freedom.

50 Several delegations (CZ, AT, LU) pointed to the need to align this with the rules in Article 77. The discussion on the exercise of data subjects rights should indeed take place in the context of Chapter VIII.

(b) (…)

(c) take all (…) measures required pursuant to Article 30;

(d) respect the conditions for enlisting another processor (…), such as a requirement of specific prior permission of the controller;

(e) (…) taking into account the nature of the processing, assist the controller in responding 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 30 to 34;

(g) return or delete, at the choice of the controller, the personal data upon the termination of the provision of data processing services specified in the contract or other legal act, unless there is a requirement to store the data under Union or Member State law to which the processor is subject;

(h) make available to the controller (…) all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits conducted by the controller.

The processor shall immediately inform the controller if, in his opinion, an instruction breaches this Regulation or Union or Member State data protection provisions.

2a. Where a processor enlists (…) another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 2 shall be imposed on that other processor *by way of a contract or other legal act under Union or Member State law*[51], in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a way that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

[51] HU suggested qualifying this reference to EU or MS law by adding 'binding that other processor to the initial processor'.

2aa. *Adherence of the processor to an approved code of conduct pursuant to Article 38 or* an approved *certification mechanism pursuant to Article 39*[52] may be used as an element to demonstrate *sufficient guarantees referred to in paragraphs 1 and 2a*.

2ab. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 2 and 2a may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 2b and 2c or on standard contractual clauses which are part of a certification granted to the controller or processor pursuant to Articles 39 and 39a.

2b. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 2 and 2a and in accordance with the examination procedure referred to in Article 87(2) [53].

2c. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 2 and 2a and in accordance with the consistency mechanism referred to in Article 57.

3. The contract or the other legal act referred to in paragraphs 2 and 2a shall be in writing, including in an electronic form.

4. (…)

5. (…)[54]

---

52 FR reservation; SK suggested specifying that where the other processor fails to fulfil its data protection obligations under such contract or other legal act, the processor shall remain fully liable to the controller for the performance of the other processor's obligation. By authorising the processor to subcontract itself and not obliging the sub-processor to have a contractual relationship with the controller, it should ensure enough legal certainty for the controller in terms of liability. The principle of liability of the main processor for any breaches of sub-processor is provided in clause 11 of Model clause 2010/87 and BCR processor and is therefore the current standard. It also suggested deleting the reference to Article 2aa.

53 PL was worried about a scenario in which the Commission would not act. CY and FR were opposed to conferring this role to COM (FR could possibly accept it for the EDPB).

54 COM reservation on deletion.

Article 27

Processing under the authority of the controller and processor

(…)

Article 28

Records of categories of personal data processing activities[55]

1. Each controller (…) and, if any, the controller's representative, 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 (…), controller's representative and data protection officer, if any;

   (b) (…)

   (c) the purposes of the processing, including the legitimate interest when the processing is based on Article 6(1)(f);

   (d) a description of categories of data subjects and of the categories of personal data relating to them;

   (e) the (…) categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries;

   (f) where applicable, the categories of transfers of personal data to a third country or an international organisation (…);

   (g) where possible, the envisaged time limits for erasure of the different categories of data.

   (h) where possible, a general description of the technical and organisational security measures referred to in Article 30(1).

[55] AT scrutiny reservation.

2a. 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, and of the controller's representative, if any;

(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 applicable, the categories of transfers of personal data to a third country or an international organisation;

(e) where possible, a general description of the technical and organisational security measures referred to in Article 30(1).

3a. 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. On request, the controller and the processor and, if any, the controller's representative, shall make the record available (…) to the supervisory authority.

4. The obligations referred to in paragraphs 1 and 2a shall not apply to:

(a) (…); or

(b) an enterprise or a body employing fewer than 250 persons, unless the processing it carries out is likely to result in a high risk for the rights and freedoms of data subject such as (…) discrimination, identity theft or fraud, [breach of (…) pseudonymity,] financial loss, damage to the reputation, loss of confidentiality of data protected by professional secrecy or any other economic or social disadvantage for the data subjects, taking into account the nature, scope, context and purposes of the processing; or

5. (…)

6. (…)

Article 29

Co-operation with the supervisory authority

(…)

SECTION 2

DATA SECURITY

Article 30

Security of processing

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, the controller and the processor shall implement appropriate technical and organisational measures[, including **(…)** pseudonymisation of personal data] to ensure a level of security appropriate to the risk.

1a. In assessing the appropriate level of security account shall be taken in particular of the risk**s** that are presented by data processing (…), in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

2. (…)

2a. Adherence to approved codes of conduct pursuant to Article 38 or an approved certification mechanism pursuant to Article 39 may be used as an element to *demonstrate compliance with the requirements set out in paragraph 1*.

2b. The controller and processor shall take steps to ensure that any person acting under the authority of the controller or the processor who has access to personal data shall not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

3. (…)

4. (…)

Article 31

Notification of a personal data breach to the supervisory authority[56]

1. In the case of a personal data breach which is likely to result in a high risk for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, [breach of (…) pseudonymity], damage to the reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 51. 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 to the data subject is not required under Article 32(3)(a) and (b)[57].

2. (…) The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

[56] AT and SI scrutiny reservation. COM reservation: the consistency with the E-Privacy Directive regime should be safeguarded; SI thought this alignment could be achieved by deleting "high" before "risk" in Articles 31 and 32.

[57] BE, AT and PL thought this paragraph should be deleted.

3. The notification referred to in paragraph 1 must at least:

(a) describe the nature of the personal data breach including, where possible and appropriate, the approximate categories and number of data subjects concerned and the categories and approximate number of data records concerned;

(b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained;

(c) (…)

(d) describe the likely consequences of the personal data breach identified by the controller;

(e) describe the measures taken or proposed to be taken by the controller to address the personal data breach; and

(f) where appropriate, indicate measures to mitigate the possible adverse effects of the personal data breach.

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.

4. The controller shall document any personal data breaches referred to in paragraphs 1 and 2, 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. (…).

5. (…)

6. (….)[58]

[58] COM reservation on deletion.

Article 32

Communication of a personal data breach to the data subject[59]

1. When the personal data breach is likely to result in a high risk for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, damage to the reputation, [breach of (…) pseudonymity], loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage, 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), (e) and (f) of Article 31(3).

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 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 case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner; or

[59] AT scrutiny reservation. COM reservation: the consistency with the E-Privacy Directive regime should be safeguarded.

d. it would adversely affect a substantial public interest.

4. (…)

5. (…)

6. (…)[60]

SECTION 3

DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

Article 33

Data protection impact assessment [61]

1. Where a type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high[62] risk for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, damage to the reputation, [breach of **(…)** pseudonymity], loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage, the controller (…)[63] shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. (…).

1a. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

---

60 COM reservation on deletion.

61 FR, HU, AT and COM expressed doubts on the concept of new types of processing, which is now clarified in recital 70. UK thought this obligation should not apply where there is an overriding public interest for the processing to take place (such as a public health emergency).

62 FR, RO, SK and UK warned against the considerable administrative burdens flowing from the proposed obligation. The UK considers that any requirements to carry out a data protection impact assessment should be limited to those cases where there is an identified high risk to the rights of data subjects.

63 COM reservation on deletion.

2. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the following cases:

(a) a systematic and extensive evaluation (…) of personal aspects relating to (…) natural persons (…), which is based on profiling and on which decisions[64] are based that produce legal effects concerning data subjects or severely affect data subjects;

(b) processing of special categories of personal data under Article 9(1) (…)[65], biometric data or data on criminal convictions and offences or related security measures, where the data are processed for taking (…) decisions regarding specific individuals on a large scale ;

(c) monitoring publicly accessible areas *on a large scale*, especially when using optic-electronic devices (…);

(d) (…);

(e) (…)[66].

2a. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the European Data Protection Board. [67]

64 In the future this wording will be aligned to the eventual wording of Article 20.

65 HU suggested that data pertaining to children be also reinserted.

66 FR scrutiny reservation. PL thought a role could be given to the EDPB in order to determine high-risk operations.

67 CZ reservation.HU wondered what kind of legal consequences, if any, would be triggered by the listing of a type of processing operation by a DPA with regard to on-going processing operations as well as what its territorial scope would be. In the view of the Presidency any role for the EDPB in this regard should be discussed in the context of Chapter VII.

2b. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the European Data Protection Board.

2c. Prior to the adoption of the lists referred to in paragraphs 2a and 2b the competent supervisory authority shall apply the consistency mechanism referred to in Article 57 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union. [68]

3. The assessment shall contain at least a general description of the envisaged processing operations, an evaluation of the risk referred to in paragraph 1, the measures envisaged to address the risk including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned[69].

3a. Compliance with approved codes of conduct referred to in Article 38 by the relevant controllers or processors shall be taken into due account in assessing lawfulness and impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment[70].

4. *The controller shall seek the views of data subjects or their representatives on the intended processing,* without prejudice to the protection of commercial or public interests or the security of the processing operations (…)[71].

---

68 CZ reservation.

69 FR scrutiny reservation.

70 HU thought this should be moved to a recital.

71 CZ and FR indicated that this was a completely impractical obligation; IE reservation.

5. (…) Where the processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or the law of the Member State to which the controller is subject, and such law regulates the specific processing operation or set of operations in question[72], paragraphs 1 to 3 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.

6. (…)

7. (…)

Article 34

Prior (…) consultation[73]

1. (…)

2. The controller (…)[74] shall consult the supervisory authority prior to the processing of personal data where a data protection impact assessment as provided for in Article 33 indicates that the processing would result in a high (…) risk in the absence of measures *to be taken by the controller* to mitigate the risk..

[72] BE and SI stated that this will have to be revisited in the context of the future debate on how to include the public sector in the scope of the Regulation.

[73] HU scrutiny reservation; SK reservation on giving this role to DPAs, which may not be able to deal with these consultations in all cases. ES proposed to exempt controllers from the obligation of a prior consultation in case they had appointed a DPO.

[74] COM and LU reservation on deleting processor.

3. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 2 would not comply with this Regulation, in particular where the controller has insufficiently identified or mitigated *the risk*, it shall within a maximum period of 6 weeks following the request for consultation give advice to the data controller , in writing, and may use any of its powers referred to in[75] Article 53 (…). This period may be extended for a further six weeks, 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.

4. (…)

5. (…)

6. When consulting the supervisory authority pursuant to paragraph 2, the controller (…) shall provide the supervisory authority, with

   (a) where applicable, the respective responsibilities of controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;

   (b) the purposes and means of the intended processing;

   (c) the measures and safeguards provided to protect the rights and freedoms of data subject**s** pursuant to this Regulation;

   (d) where applicable , the contact details of the data protection officer;

   (e) the data protection impact assessment as provided for in Article 33 and

   (f) any (…) other information requested by the supervisory authority (…).

[75] UK reservation; it thought the power to prohibit processing operations should not apply during periods in which there is an overriding public interest for the processing to take place (such as a public health emergency). The Presidency thinks this issue should however be debated in the context of Chapter VI on the powers of the DPA, as these may obviously also be used regardless of any consultation.

7. Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure adopted by a national parliament or of a regulatory measure based on such a legislative measure which provide for the processing of personal data (…)[76].

7a. Notwithstanding paragraph 2, Member States' law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to the processing of personal data by a controller for the performance of a task carried out by the controller in the public interest, including the processing of such data in relation to social protection and public health[77].

8. (…)

9. (…)

[76] IE scrutiny reservation on deletion.
[77] SE scrutiny reservation.

SECTION 4
DATA PROTECTION OFFICER

Article 35

Designation of the data protection officer

1. The controller or the processor may, or where required by Union or Member State law shall,[78] designate a data protection officer (…).

2. A group of undertakings may appoint a single data protection officer.

3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

4. (…).

5. 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 37, particularly the absence of any conflict of interests. (…).

6. (…)

7. (…). During their term of office, the data protection officer may, apart from serious grounds under the law of the Member State concerned which justify the dismissal of an employee or civil servant, be dismissed only if the data protection officer no longer fulfils the conditions required for the performance of his or her tasks pursuant to Article 37.

[78] Made optional further to decision by the Council. AT scrutiny reservation. DE, HU and AT would have preferred to define cases of a mandatory appointment of DPA in the Regulation itself and may want to revert to this issue at a later stage. COM reservation on optional nature and deletion of points a) to c).

8. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

9. The controller or the processor shall publish the contact details of the data protection officer and communicate these to the supervisory authority (…).

10. Data subjects may contact the data protection officer on all issues related to the processing of the data subject's data and the exercise of their rights under this Regulation.

11. (…)

Article 36

Position of the data protection officer

1. The controller or the processor shall ensure that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.

2. The controller or the processor shall support the data protection officer in performing the tasks referred to in Article 37 by providing (…) resources necessary to carry out these tasks as well as access to personal data and processing operations.

3. The controller or processor shall ensure that the data protection officer can act in an independent manner with respect to the performance of his or her tasks and does not receive any instructions regarding the exercise of these tasks. He or she shall not be penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

4. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

Article 37

Tasks of the data protection officer

1. The (…) data protection officer (…) shall have the following tasks:

(a) to inform and advise the controller or the processor and the employees who are processing personal data of their obligations pursuant to this Regulation and other Union or Member State data protection provisions (…);

(b) to monitor compliance with this Regulation, 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) (…)

(d) (…)

(e) (…)

(f) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 33;

(g) to monitor 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 of personal data, including the prior consultation referred to in Article 34, and consult, as appropriate, on any other matter.

2. (…)

2a. The data protection officer shall in the performance his or her tasks have due regard to the risk associated with the processing operations, taking into account the *nature, scope, context and purposes* of the processing.

SECTION 5
CODES OF CONDUCT AND CERTIFICATION

Article 38

Codes of conduct [79]

1. The Member States, the supervisory authorities, the European Data Protection Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors and the specific needs of micro, small and medium-sized enterprises.

1a. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of provisions of this Regulation, such as:

(a) fair and transparent data processing;

(aa) the legitimate interests pursued by controllers in specific contexts;

(b) the collection of data;

(bb) the pseudonymisation of personal data;

(c) the information of the public and of data subjects;

(d) the exercise of the rights of data subjects;

(e) information and protection of children and the way to collect the parent's and guardian's consent;

(ee) measures and procedures referred to in Articles 22 and 23 and measures to ensure security of processing referred to in Article 30;

(ef) notification of personal data breaches to supervisory authorities and communication of such breaches to data subjects;

(f) (…).

1ab. In addition to adherence by controller or processor subject to the regulation, codes of conduct *approved* pursuant to paragraph 2 may also be adhered to by controllers or processors that are not subject to this Regulation according to Article

[79] AT, FI, SK and PL scrutiny reservation.

3 in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organisations under the terms referred to in Article 42(2)(d). Such controllers or processors shall make binding and enforceable commitments, via contractual instruments or otherwise, to apply those appropriate safeguards including as regards data subjects' rights.

1b. Such a code of conduct shall contain mechanisms which enable the body referred to in paragraph 1 of article 38a to carry out the mandatory[80] monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of the supervisory authority which is competent pursuant to Article 51 or 51a.

2. Associations and other bodies referred to in paragraph 1a which intend to prepare a code of conduct, or to amend or extend an existing code, shall submit the draft code to the supervisory authority which is competent pursuant to Article 51. The supervisory authority shall give an opinion on whether the draft code, or amended or extended code, is in compliance with this Regulation and shall approve such draft, amended or extended code if it finds that it provides sufficient appropriate safeguards.

2a. Where the opinion referred to in paragraph 2 confirms that the code of conduct, or amended or extended code, is in compliance with this Regulation and the code is approved, and if the code of conduct does not relate to processing activities in several Member States, the supervisory authority shall register the code and publish the details thereof.

[80] CZ preferred this monitoring to be optional.

2b. Where the draft code of conduct relates to processing activities in several Member States, the supervisory authority competent pursuant to Article 51 shall, before approval, submit it in the procedure referred to in Article 57 to the European Data Protection Board which shall give an opinion on whether the draft code, or amended or extended code, is in compliance with this Regulation or, in the situation referred to in paragraph 1ab, provides appropriate safeguards[81].

3. Where the opinion referred to in paragraph 2b confirms that the code of conduct, or amended or extended code, is in compliance with this Regulation, or, in the situation referred to in paragraph 1ab, provides appropriate safeguards ,the European Data Protection Board shall submit its opinion to the Commission.

4. The Commission may adopt implementing acts for deciding that the approved codes of conduct and amendments or extensions to existing approved codes of conduct submitted to it pursuant to paragraph 3 have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

5. The Commission shall ensure appropriate publicity for the approved codes which have been decided as having general validity in accordance with paragraph 4.

5a. The European Data Protection Board shall collect all approved codes of conduct and amendments thereto in a register and shall make them publicly available through any appropriate means, such as through the European E-Justice Portal.

Article 38a

Monitoring of approved codes of conduct[82]

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 52 and 53, the monitoring of compliance with a code of conduct pursuant to Article 38 (1b), may be carried out by a body[83] which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for this purpose by the competent supervisory authority.

2. A body referred to in paragraph 1 may be accredited for this purpose if:

---

81 FR made a proposal for a paragraph 2c: 'Approved codes of conduct pursuant to paragraph 2a shall constitute an element of the contractual relationship between the controller and the data subject. When such codes of conduct determine the compliance of the controller or processor with this Regulation, they shall be legally binding and enforceable.'

82 AT, LU scrutiny reservation.

83 CZ, ES, LU are opposed to giving this role to such separate bodies. Concerns were raised, *inter alia*, on the administrative burden involved in the setting up of such bodies. Codes of conduct are an entirely voluntary mechanism in which no controller is obliged to participate.

(a) it has demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;

(b) it has established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;

(c) it has established procedures and structures to deal with complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make these procedures and structures transparent to data subjects and the public;

(d) it demonstrates to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

3. The competent supervisory authority shall submit the draft criteria for accreditation of a body referred to in paragraph 1 to the European Data Protection Board pursuant to the consistency mechanism referred to in Article 57.

4. Without prejudice to the provisions of Chapter VIII, a body referred to in paragraph 1 may, subject to adequate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the competent supervisory authority of such actions and the reasons for taking them.

5. The competent supervisory authority shall revoke the accreditation of a body referred to in paragraph 1 if the conditions for accreditation are not, or no longer, met or actions taken by the body are not in compliance with this Regulation.

6. This article shall not apply to the processing of personal data carried out by public authorities and bodies.

Article 39

Certification[84]

1. The Member States, the European Data Protection Board and the Commission shall encourage, in particular at Union level, the establishment of data protection

[84] AT, FR, FI scrutiny reservation. FR thought the terminology used was unclear an that the DPA should be in a position to check compliance with certified data protection policies; this should be clarified in Article 53.

certification mechanisms and of data protection seals and marks for the purpose of demonstrating compliance with this Regulation of processing operations carried out by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.

1a. In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks *approved* pursuant to paragraph 2a may also be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation according to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in Article 42(2)(e). Such controllers or processors shall make binding and enforceable commitments, via contractual instruments or otherwise, to apply those appropriate safeguards, including as regards data subjects' rights.

2. A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authority which is competent pursuant to Article 51 or 51a.

2a. A certification pursuant to this Article shall be issued *by the* certification *bodies referred to in Article 39a, or where applicable, by the competent supervisory authority* on the basis of the criteria approved by the competent supervisory authority or, *pursuant to Article 57*, the European Data Protection Board[85].

3. The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 39a, *or where applicable, the competent supervisory authority,* with all information and access to its processing activities which are necessary to conduct the certification procedure.

4. The certification shall be issued to a controller or processor for a maximum period of 3 years and may be renewed under the same conditions as long as the relevant requirements continue to be met. It shall be withdrawn by the certification bodies referred to in Article 39a, or where applicable, by the competent supervisory authority where the requirements for the certification are not or no longer met.

[85] This is without prejudice to the future discussion on the exact powers of the EDPB. This discussion will take place in the context of the discussion on the one-stop-shop mechanism.

5. The European Data Protection Board shall collect all certification mechanisms and data protection seals in a register and shall make them publicly available through any appropriate means, such as through the European E-Justice Portal.

Article 39a

Certification body and procedure[86]

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 52 and 53, the certification shall be issued and renewed by a certification body which has an appropriate level of expertise in relation to data protection. Each Member State shall provide whether these certification bodies are accredited by:[87]

   (a) the supervisory authority which is competent according to Article 51 or 51a; and/or

   (b) the National Accreditation Body named in accordance with Regulation (EC) 765/2008 of the European parliament and the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products in compliance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent according to Article 51 or 51a.

2. The certification body referred to in paragraph 1 may be accredited for this purpose only if:

   (a) it has demonstrated its independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;

[86] AT, FR, LU scrutiny reservation.
[87] BE scrutiny reservation.

(aa) undertaken to respect the criteria *referred to in paragraph 2a of Article 39* and approved by the supervisory authority which is competent according to Article 51 or 51a or , pursuant to Article 57, the European Data Protection Board;

(b) it has established procedures for the issue, periodic review and withdrawal of data protection seals and marks;

(c) it has established procedures and structures to deal with complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make these procedures and structures transparent to data subjects and the public;

(d) it demonstrates to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

3. The accreditation of the certification bodies referred to in paragraph 1 shall take place on the basis of criteria approved by the supervisory authority which is competent according to Article 51 or 51a or, *pursuant to Article 57*, the European Data Protection Board[88]. *In case of an accreditation pursuant to point (b) of paragraph 1, these requirements complement those envisaged in Regulation 765/2008 and the technical rules that describe the methods and procedures of the certification bodies*.

4. The certification body referred to in paragraph 1 shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this Regulation. The accreditation is issued for a maximum period of five years and can be renewed in the same conditions as long as the body meets the requirements.

5. The certification body referred to in paragraph 1 shall provide the competent supervisory authority with the reasons for granting or withdrawing the requested certification.

[88] This is without prejudice to the future discussion on the exact powers of the EDPB. This discussion will take place in the context of the discussion on the one-stop-shop mechanism.

6. *The* requirements referred to in paragraph 3*, the* criteria referred to in paragraph 2a of Article 39 *shall be made public by the supervisory authority in an easily accessible form*. The supervisory authorities shall also transmit these to the European Data Protection Board. The European Data Protection Board shall collect all certification mechanisms and data protection seals in a register and shall make them publicly available through any appropriate means, such as through the European E-Justice Portal.

6a. Without prejudice to the provisions of Chapter VIII, the competent supervisory authority or the National Accreditation Body shall revoke the accreditation it granted to a certification body referred to in paragraph 1 if the conditions for accreditation are not, or no longer, met or actions taken by the body are not in compliance with this Regulation[89].

7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86, for the purpose of (…) specifying the criteria and requirements to be taken into account for the data protection certification mechanisms referred to in paragraph 1, [including conditions for granting and revocation, and requirements for recognition of the certification and the requirements for a standardised 'European Data Protection Seal' within the Union and in third countries].

7a. The European Data Protection Board shall give an opinion to the Commission on the criteria and requirements referred to in paragraph 7[90].

8. The Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2)[91].

---

89 CZ, FR and HU though the national accreditation body should always consult the DPA before accrediting a certification body.

90 This is without prejudice to the future discussion on the exact powers of the EDPB. This discussion will take place in the context of the discussion on the one-stop-shop mechanism.

91 DE pleaded in favour of deleting the last two paragraphs and suggested adding a new paragraph: "The previous paragraphs shall not affect provisions governing the responsibility of national certification bodies, the accreditation procedures and the specification of criteria for security and data protection. Commission's power to adopt acts pursuant to paragraphs 7 and 8 shall not apply to national and international certification procedures carried out on this basis. Security certificates issued by the responsible bodies or bodies accredited by them in the framework of these procedures shall be mutually recognized." ES also thought that this should not be left exclusively to the Commission.

CHAPTER V
TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS[92] [93] [94] [95]

Article 40

General principle for transfers

(…)

[92] In light of the fact that the public interest exception would in many cases be the main ground warranting an international transfer of personal data, some delegations (CZ, DE, LV, UK) queried whether the 'old' adequacy principle/test should still maintained and set out in such detail, as it would in practice not be applied in that many cases. DE in particular thought that the manifold exceptions emptied the adequacy rule of its meaning. Whilst they did not disagree with the goal of providing protection against transfer of personal data to third countries, it doubted whether the adequacy principle was the right procedure therefore, in view of the many practical and political difficulties (the latter especially regarding the risk of a negative adequacy decision, cf. DE, FR, UK). The feasibility of maintaining an adequacy-test was also questioned with reference to the massive flows of personal data in in the context of cloud computing: BG, DE, FR, IT, NL, SK and UK. FR and DE asked whether a transfer of data in the context of cloud computing or the disclosure of personal data on the internet constitutes an international transfer of data. DE also thought that the Regulation should create a legal framework for 'Safe Harbor-like' arrangements under which certain guarantees to which companies in a third country have subscribed on a voluntary basis are monitored by the public authorities of that country. The applicability to the public sector of the rules set out in this Chapter was questioned (EE), as well as the delimitation to the scope of proposed Directive (FR). The impact of this Chapter on existing Member State agreements was raised by several delegations (FR, PL).

[93] NL and UK pointed out that under the 1995 Data Protection Directive the controller who wants to transfer data is the first one to assess whether this possible in under the applicable (EU) law and they would like to maintain this basic principle, which appears to have disappeared in the Commission proposal.

[94] DE asked which law would apply to data transferred controllers established in third countries that come within the ambit of Article 3(2); namely whether this would be EU law in accordance with that provision.

[95] AT has made a number of proposals regarding this chapter set out in 10198/14 DATAPROTECT 82 JAI 363 MI 458 DRS 73 DAPIX 71 FREMP 103 COMIX 281 CODEC 1351.

Article 41

Transfers with an adequacy decision[96]

1. A transfer of personal data to a third country or an international organisation may take place where the Commission[97] has decided that the third country, or a territory or one ore more specified sectors 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. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

   (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation (…)[98], both general and sectoral, data protection rules and security measures, including rules for onward transfer of personal data to another third country or international organisation, which are complied with in that third country or 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 (…)[99];

---

96 Some delegations raised concerns on the time taken up by adequacy procedures and stressed the need to speed up this process. COM stated that this should not be at the expense of the quality of the process of adequacy.

97 CZ, DE and SI reservation on giving such power to the Commission. NL and UK indicated that on this point the proposal seemed to indicate a shift from the 1995 Data Protection Directive, which put the responsibility for assessing a third country's data protection legislation in the first place with the controller who wanted to transfer personal data. UK had considerable doubts on the feasibility of the list in paragraph 2.

98 AT would have preferred including a reference to national security.

99 NL thought that Article 41 was based on fundamental rights and legislation whereas Safe harbour is of a voluntary basis and that it was therefore useful to set out elements of Safe Harbour in a separate Article. DE asked how Safe Harbour could be set out in Chapter V.

(b) the existence and effective functioning of one or more independent supervisory authorities[100] 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 the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States;

(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[101] 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, after assessing the adequacy[102] of the level of protection, may decide that a third country, or a territory or one or more specified sector within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. (…)[103]. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the (independent) supervisory authority(ies)

---

100 NL queried how strict this independence would need to be assessed. BE suggested adding a reference to independent judicial authorities, FI suggested to refer to 'authorities' *tout court*.

101 CZ would prefer stronger language on the COM obligation to request an opinion from the EDPB.

102 CZ, RO and SI reservation on giving such power to the Commission. DE thought that stakeholders should be involved in this process. NL and UK indicated that on this point the proposal seemed to indicate a shift from the 1995 Data Protection Directive, which put the responsibility for assessing a third country's data protection legislation in the first place with the controller who wanted to transfer personal data.

103 CZ, DE DK, HR, IT, NL, PL, SK and RO thought an important role should be given to the EDPB in assessing these elements.COM has pointed out that there can be no additional step in the Comitology procedure, in order to be in line with the Treaties and Regulation 182/2011.

mentioned in point (b) of paragraph 2. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 87(2)[104].

3a. *Decisions adopted by the Commission on the basis of Article 25(6)* (…) *of Directive 95/46/EC shall remain in force until amended, replaced or repealed by the Commission*[105] in accordance with the examination procedure referred to in Article 87(2)[106].

[104] DE queried the follow-up to such decisions and warned against the danger that third countries benefiting from an adequacy decision might not continue to offer the same level of data protection. COM indicated there was monitoring of third countries for which an adequacy decision was taken.

[105] Moved from paragraph 8. CZ and AT thought an absolute maximum time period should be set (sunset clause), to which COM was opposed. NL, PT and SI thought this paragraph 3a was superfluous or at least unclear. Also RO thought that, if maintained, it should be moved to the end of the Regulation.

[106] DE and ES suggested to request the Board for an opinion. COM has pointed out that there can be no additional step in the Comitology procedure, in order to be in line with the Treaties and Regulation 182/2011. DE asked if a decision in paragraph 3a lasted forever. IE considered paragraph 3a providing necessary flexibility. CZ thought that new States should not be disadvantaged compared to those having received an adequacy decision under Directive 1995.

4. (…)

4a. The Commission shall monitor the functioning of decisions adopted pursuant to paragraph 3 and decisions adopted on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC[107].

5. The Commission may decide 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 87(2) or, in cases of extreme urgency (…), in accordance with the procedure referred to in Article 87(3)[108].

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.

6. A decision pursuant to paragraph 5 is without prejudice to transfers of personal data to the third country, or the territory or specified sector within that third country, or the international organisation in question pursuant to Articles 42 to 44[109].

---

107 BE queried about the reference to the 1995 Directive. CZ perceives this as superfluous.

108 FR and UK suggested the EDPB give an opinion before COM decided to withdraw an adequacy decision.

109 DE asked for the deletion of paragraph 6. DK thought the moment when third countries should be consulted was unclear.

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, 3a and 5.

8. (…)

Article 42

Transfers by way of appropriate safeguards[110]

1. In the absence of a decision pursuant to paragraph 3 of Article 41, a controller or processor may transfer personal data to (…) a third country or an international organisation only if the controller or processor has adduced appropriate safeguards, also covering onward transfers (…) .

2. The appropriate safeguards referred to in paragraph 1 *may* be provided for (…), without requiring any specific authorisation from a supervisory authority, by:

   (oa) a legally binding **and enforceable** instrument **between public authorities or bodies**[111]; or

   (a) binding corporate rules referred to in Article 43; or

   (b) standard data protection clauses adopted by the Commission (…) in accordance with the examination procedure referred to in Article 87(2)**[112]**; or

   (c) standard data protection clauses adopted by a supervisory authority and adopted by the Commission pursuant to the examination procedure referred to in Article 87(2).

---

110 UK expressed concerns regarding the length of authorisation procedures and the burdens these would put on DPA resources. The use of these procedures regarding data flows in the context of cloud computing was also questioned.

111 HU has serious concerns; the proposed general clause ("a legally binding instrument") is too vague because the text does not define its content. Furthermore, the text does not provide for previous examination by the DPA either. HU therefore suggests either deleting this point or subjecting such instrument to the authorisation of the DPA, as it believes that there is a real risk that transfers based on such a vague instrument might seriously undermine the rights of the data subjects.

112 FR reservation on the possibility for COM to adopt such standard clauses.

(d) an approved code of conduct pursuant to Article 38 together with binding and enforceable commitments of the controller or processor (…) in the third country to apply the appropriate safeguards, **including as regards data subjects' rights** ; or

(e) an approved certification mechanism pursuant to Article 39 together with binding and enforceable commitments of the controller or processor (…) in the third country to apply the appropriate safeguards, **including as regards data subjects' rights**.

2a. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:

(a) contractual clauses between the controller or processor and the controller, processor or the recipient of the data (…) in the third country or international organisation; or

(b) (…)

(c) (…)

(d) provisions to be inserted into administrative arrangements between public authorities or bodies (…).

3. (….)

4. (….)

5a. The supervisory authority shall apply the consistency mechanism in the cases referred to in points (ca), (d), (e) and (f) of Article 57 (2).

5b. *Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed*

by that supervisory authority[113]. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by the Commission[114] in accordance with the examination procedure referred to in Article 87(2)[115].

Article 43

Binding corporate rules[116]

1. The competent supervisory authority shall *approve*[117] *binding corporate rules* in accordance with the consistency mechanism set out in Article 57 provided that they:

   (a) are legally binding and apply to, and are enforced by, every member concerned of the group of undertakings or group of enterprises engaged in a joint economic activity;

---

113 UK and ES disagreed with the principle of subjecting non-standardised contracts to prior authorisation by DPAs. IT was thought that this was contrary to the principle of accountability. DE emphasised the need of monitoring.

114 AT thought an absolute time period should be set.

115 DE and ES have suggested to request the Board for an opinion. COM has pointed out that there can be no additional step in the Comitology procedure, in order to be in line with the Treaties and Regulation 182/2011.

116 NL thought it should be given a wider scope. BE and NL pointed to the need for a transitional regime allowing to 'grandfather' existing BCRs. NL asked whether the BCRs should also be binding upon employees. SI thought BCRs should also be possible with regard to some public authorities, but COM stated that it failed to see any cases in the public sector where BCRs could be applied. HU said that it thought that BCRs were used not only by profit-seeking companies but also by international bodies and NGOs.

117 DE and UK expressed concerns on the lengthiness and cost of such approval procedures. The question was raised which DPAs should be involved in the approval of such BCRs in the consistency mechanism.

(b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data;

(c) fulfil the requirements laid down in paragraph 2.

2. The binding corporate rules referred to in paragraph 1 shall specify at least:

(a) the structure and contact details of the *concerned* group and of each of its members;

(b) the data transfers or categories of transfers, including the types of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;

(c) their legally binding nature, both internally and externally;

(d) application of the general data protection principles, in particular purpose limitation, (…) data quality, legal basis for the processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies (…) not bound by the binding corporate rules;

(e) the rights of data subjects in regard to the processing of their personal data and the means to exercise these rights, including the right not to be subject to (…) profiling in accordance with Article 20, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor may only be exempted from this liability, in whole or in part, on proving that that member is not responsible for the event giving rise to the damage[118];

[118] DE thought that the reference to exemptions should be deleted here.

(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in accordance with Articles 14 and 14a;

(h) the tasks of any data protection officer designated in accordance with Article 35 or any other person or entity in charge of the monitoring (…) compliance with the binding corporate rules within the group, as well as monitoring the training and complaint handling;

(hh) the complaint procedures;

(i) the mechanisms within the group, for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred under point h) and to the board of the controlling undertaking or of the group of enterprises, and should be available upon request to the competent supervisory authority;

(j) the mechanisms for reporting and recording changes to the rules and reporting these changes to the supervisory authority;

(k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group (…), in particular by making available to the supervisory authority the results of (…) verifications of the measures referred to in point (i) of this paragraph[119];

(l) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules[120]; and

[119] BE suggested making this more explicit in case of a conflict between the 'local' legislation applicable to a member of the group and the BCR.

[120] CZ expressed concerns about the purpose of this provision and its application. UK found this point very prescriptive and wanted BCRs to be flexible to be able to be used for different circumstances.

(m) the appropriate data protection training to personnel having permanent or regular access to personal data (...).

2a. The European Data Protection Board shall advise the Commission on the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules.

[3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for binding corporate rules within the meaning of this Article, in particular as regards the criteria for their approval, the application of points (b), (d), (e) and (f) of paragraph 2 to binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned.][121]

4. The Commission may specify the format and procedures for the exchange of information (…) between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

[121] CZ, IT, SE and NL reservation. FR scrutiny reservation regarding (public) archives. RO and HR thought the EDPB should be involved. PL and COM wanted to keep paragraph 3.

Article 44

Derogations for specific situations[122]

1. In the absence of an adequacy decision pursuant to paragraph 3 of Article 41, or of appropriate safeguards pursuant to Article 42, including binding corporate rules, 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:

   (a) the data subject has explicitly[123] consented to the proposed transfer, after having been informed that such transfers may involve *risks* for the data subject due to the absence of an adequacy decision and appropriate safeguards; or

   (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or

   (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or

   (d) the transfer is necessary for important reasons of public interest[124]; or

   (e) the transfer is necessary for the establishment, exercise or defence of legal claims; or

---

122 EE reservation. NL parliamentary reservation. CZ, EE and UK and other delegations that in reality these 'derogations' would become the main basis for international data transfers and this should be acknowledged as such by the text of the Regulation.

123 UK thought the question of the nature of the consent needed to be discussed in a horizontal manner.

124 DE remarked that the effects of (d) in conjunction with paragraph 5 need to be examined, in particular with respect to the transfer of data on the basis of court judgments and decisions by administrative authorities of third states, and with regard to existing mutual legal assistance treaties. IT reservation on the (subjective) use of the concept of public interest. HR suggested adding 'which is not overridden by the legal interest of the data subject'.

(f) the transfer is necessary in order to protect the vital interest of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or

(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest but only to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case; or

(h) the transfer, *which* is not large scale or *frequent*[125], is necessary for the purposes of legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject and where the controller (…) has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and (…) based on this assessment adduced suitable safeguards[126] with respect to the protection of personal data.

2. A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. When the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

[125] AT, ES, HU, MT, PL, PT and SI would prefer to have this derogation deleted as they think it is too wide; it was stated that data transfers based on the legitimate interest of the data controller and directed into third countries that do not provide for an adequate level of protection with regard to the right of the data subjects would entail a serious risk of lowering the level of protection the EU acquis currently provides for.) DE and ES scrutiny reservation on the terms 'frequent or massive'. DE, supported by SI, proposed to narrow it by referring to 'overwhelming legitimate interest'. ES proposed to replace it by 'are small-scale and occasional'; UK asked why it was needed to add another qualifier to the legitimate interest of the transfer and thought that such narrowing down of this derogation was against the risk-based approach.

[126] AT and NL reservation: it was unclear how this reference to appropriate safeguards relates to appropriate safeguards in Article 42.

3. (…)

4. Points (a), (b), (c) and (h) of paragraph 1shall not apply to activities carried out by public authorities in the exercise of their public powers[127].

5. The public interest referred to in point (d) of paragraph 1 must be recognised in Union law or in the national law of the Member State to which the controller is subject.

5a. In the absence of an adequacy decision, Union law or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation[128]. Member States shall notify such provisions to the Commission[129].

6. The controller or processor shall document the assessment as well as the suitable safeguards (…) referred to in point (h) of paragraph 1 in the records referred to in Article 28 (…).

6a. (…)

7. (…)

[127] BE scrutiny reservation. FR has a reservation concerning the exception of public authorities.

[128] SI and UK scrutiny reservation. FR and ES proposed that this provision should be included in another provision.

[129] Some delegations (FR, PL, SI) referred to the proposal made by DE (for new Article 42a: 12884/13 DATAPROTECT 117 JAI 689 MI 692 DRS 149 DAPIX 103 FREMP 116 COMIX 473 CODEC 186) and the amendment voted by the European Parliament (Article 43a), which will imply discussions at a later stage.

Article 45

International co-operation for the protection of personal data[130]

1. In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:

   (a) develop international co-operation mechanisms to facilitate the *effective* enforcement of legislation for the protection of personal data;

   (b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through (…) complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms[131];

   (c) engage relevant stakeholders in discussion and activities aimed at promoting international co-operation in the enforcement of legislation for the protection of personal data;

   (d) promote the exchange and documentation of personal data protection legislation and practice.

2. (…)

---

130 PL thought (part of) Article 45 could be inserted into the preamble. NL, RO and UK also doubted the need for this article in relation to adequacy and thought that any other international co-operation between DPAs should be dealt with in Chapter VI. NL thought this article could be deleted. ES has made an alternative proposal, set out in 6723/6/13 REV 6 DATAPROTECT 20 JAI 130 MI 131 DRS 34 DAPIX 30 FREMP 15 COMIX 111 CODEC 394.

131 AT and FI thought this subparagraph was unclear and required clarification.

[NOT YET AGREED:

Chapter VI: Supervisory authorities

Chapter VII: Cooperation and consistency

Chapter VIII: Remedies, Liability and sanctions]

CHAPTER IX
PROVISIONS RELATING TO SPECIFIC DATA PROCESSING SITUATIONS

Article 80

Processing of personal data and freedom of expression and information

1. The national law of the Member State shall (…) reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including the processing of personal data for journalistic purposes and the purposes of academic, artistic or literary expression.

2. For *the processing of personal data carried out for journalistic purposes or the purpose of academic artistic or literary expression*, Member States shall[132] provide for exemptions or derogations from the provisions in Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organizations), Chapter VI (independent supervisory authorities), Chapter VII (co-operation and consistency)[133] if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information (…).

---

[132] HU, AT, SI and SE reservation; they would prefer not to limit this paragraph to journalistic processing.

[133] BE, DE, FR, IE and SE had requested to include also a reference to Chapter VIII. This was opposed to by COM. The Presidency points out that in case the freedom of expression prevails over the right to data protection, there will obviously no infringement to sanction. Where an infringement is found to have place, the interference with the freedom of expression will have to taken into account as an element in the determination of the sanction. This application of the proportionality principle should be reflected in Chapter VIII.

Article 80a

Processing of personal data and public access to official documents [134]

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 pursuant to this Regulation.

Article 80aa

Processing of personal data and reuse of public sector information

Personal data in in public sector information 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 the reuse of such official documents and public sector information with** *the right to the protection of personal data pursuant to this Regulation*[135].

Article 80b [136]

Processing of national identification number

Member States may determine the specific conditions for the processing of a national identification number or any other identifier of general application. In this case the national identification number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.

---

134 SK and PT scrutiny reservation.

135 COM reservation in view of incompatibility with existing EU law, in particular Directive 2003/98/EC (as amended by Directive 2013/37/EU).

136 DK, PL, SK scrutiny reservation.

Article 81

Processing of personal data for health -related purposes

(…)[137]

Article 81a

Processing of genetic data

(…)[138]

Article 82

Processing in the employment context

1. Member States may by law or by collective agreements, provide for more specific[139] rules to ensure the protection of the rights and freedoms in respect of 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 agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property 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. (…)

2. [Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them].

---

137 See Article 9(2)(g),(h), (hb) and (4) which enshrine the basic idea, previously expressed in Article 81, that sensitive data may be processed for purposes of medicine, health-care, public health and other public interests, subject to certain appropriate safeguards based on Union law or Member State law. This text is not part of the partial general approach which the Council is asked to agree at its meeting of 4 December 2014 and will be subject to further scrutiny at technical level.

138 See Article 9(2)(ha) and (4) which enshrine the basic idea, previously expressed in Article 81a, that genetic data may be processed, e.g. for medical purposes or to clarify parentage, subject to certain appropriate safeguards based on Union law or Member State law. This text is not part of the partial general approach which the Council is asked to agree at its meeting of 4 December 2014 and will be subject to further scrutiny at technical level.

139 DE, supported, by AT, CZ, HU, DK and SI, wanted to refer to 'stricter' rules.

3. Member States may by law determine the conditions under which personal data in the employment context may be processed on the basis of the consent of the employee[140].

Article 82a

Processing for purposes of social protection

(…)

Article 83

Derogations applying to processing of personal data for archiving, scientific, statistical and historical purposes

1. Where personal data are processed for scientific, statistical[141] or historical purposes Union or Member State law may, subject to appropriate safeguards for the rights and freedoms of the data subject, provide for derogations from Articles 14a(1) and (2), 15, 16, 17, 17a, 17b, 18 and 19[142], insofar as such derogation is necessary for the fulfilment of the specific purposes.

1a. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may, subject to appropriate safeguards for the rights and freedoms of the data subject, provide for derogations from Articles 14a(1) and (2), 15, 16, 17, 17a, 17b, 18, 19, 23, 32, 33 and 53 (1b)(d) and (e), insofar as such derogation is necessary for the fulfilment of these purposes[143].

1b. In case a type of processing referred to in paragraph**s** 1 and 1a serves at the same time another purpose, the derogations allowed for apply only to the processing for the purposes referred to in those paragraphs.

---

140 This paragraph may need to be looked at again in the context of the discussions on Articles 7 and 8 for consent. COM, PL, PT scrutiny reservation.

141 PL and SI would want to restrict this to statistical processing in the public interest.

142 NL and DK proposed adding a reference to Article 7. SI supported this as far as scientific processing is concerned. PL suggested deleting the reference to Article 19.

143 COM and AT thought the list of articles from which can be derogated should be more limited.

2. The appropriate safeguards referred to in paragraphs 1 and 1a shall be laid down in Union or Member State law and be such to ensure that technological and/or organisational protection measures pursuant to this Regulation are applied to the personal data (…), to minimise the processing of personal data in pursuance of the proportionality and necessity principles, such as *pseudonymising the data,* unless those measures prevent achieving the purpose of the processing and such purpose cannot be otherwise fulfilled within reasonable means.

3. (…).

Article 84

Obligations of secrecy [144]

1. (…) Member States may adopt specific rules to set out the (…) powers by the supervisory authorities laid down in points (da) and (db) of Article 53(1) in relation to controllers or processors that are subjects under Union or Member State law or rules established by national competent bodies to an obligation of professional secrecy**,** other equivalent obligations of secrecy or to a code of professional ethics supervised and enforced by professional bodies, where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. These rules shall only apply with regard to personal data which the controller or processor has received from or has obtained in an activity covered by this obligation of secrecy.

2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

[144] DE and UK scrutiny reservation.

Article 85

Existing data protection rules of churches and religious associations[145]

1. Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of individuals with regard to the processing of personal data, such rules may continue to apply, provided that they are brought in line with the provisions of this Regulation.

2. Churches and religious associations which apply comprehensive rules in accordance with paragraph 1, shall be subject to the control of an independent supervisory authority which may be specific, provided that it fulfils the conditions laid down in Chapter VI of this Regulation.

[NOT YET AGREED:

Chapter X: Delegated Acts and Implementing Acts

Chapter XI: Final Provisions]

---

[145] MT, NL, AT and PT reservation.