



Council of the
European Union

Brussels, 24 October 2014
(OR. en)

14270/1/14
REV 1

LIMITE

DATAPROTECT 138
JAI 773
MI 775
DRS 127
DAPIX 142
FREMP 171
COMIX 547
CODEC 2013

Interinstitutional File:
2012/0011 (COD)

NOTE

From: Presidency
To: Working Party on Information Exchange and Data Protection
Subject: Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)
- Chapter II, Article 21 and Chapter IX

Following the discussions at the DAPIX meetings of 30 September - 1 October 2014 and of 21-22 October 2014, the Presidency has made a number of changes, which are highlighted in in the annex **in bold underlined text**.

Delegations are invited to discuss the changes with a view to preparing a partial general approach on the annexed text at the December JHA Council meeting.

- 7) The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the way data protection is implemented across the Union, legal uncertainty and a widespread public perception that there are significant risks for the protection of individuals associated notably with online activity. Differences in the level of protection of the rights and freedoms of individuals, notably to the right to the protection of personal data, with regard to the processing of personal data afforded in the Member States may prevent the free flow of personal data throughout the Union. These differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. This difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC.
- 8) In order to ensure a consistent and high level of protection of individuals and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of individuals with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. Regarding the processing of personal data by public authorities for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed maintain or introduce national provisions ensuring a higher level of protection than that provided for in this Regulation, except for those cases where this Regulation lays down specific regimes of data protection.

- 9) Effective protection of personal data throughout the Union requires strengthening and detailing the rights of data subjects and the obligations of those who process and determine the processing of personal data, but also equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent penalties for offenders in the Member States.
- 10) Article 16(2) of the Treaty mandates the European Parliament and the Council to lay down the rules relating to the protection of individuals with regard to the processing of personal data and the rules relating to the free movement of personal data.
- 11) In order to ensure a consistent level of protection for individuals throughout the Union and to prevent divergences hampering the free movement of data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide individuals in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors or at least the same minimum level of legally enforceable rights and obligations and responsibilities regarding the processing of personal data by public authorities for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, to ensure consistent monitoring of the processing of personal data, and equivalent penalties in all Member States as well as effective co-operation by the supervisory authorities of different Member States. The proper functioning of the internal market requires that the free movement of personal data within the Union should not be restricted or prohibited for reasons connected with the protection of individuals with regard to the processing of personal data. When Member States maintain or introduce more stringent national provisions ensuring a higher level of protection than that provided for in this Regulation regarding the processing of personal data by their public authorities performing a task carried out in the public interest or in the exercise of official authority vested in the controller, they should not be allowed to impose other requirements than those flowing from this Regulation regarding data provided by public authorities from another Member State nor should they be allowed to impose any other requirements than those flowing from this Regulation regarding personal data they provide to public authorities from another Member State.

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

- 12) The protection afforded by this Regulation concerns natural persons, whatever their nationality or place of residence, in relation to the processing of personal data. With regard to the processing of data which concern legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person, the protection of this Regulation should not be claimed by any such person. (...).
- 13) The protection of individuals should be technologically neutral and not depend on the techniques used; otherwise this would create a serious risk of circumvention. The protection of individuals should apply to processing of personal data by automated means as well as to manual processing, if the data are contained or are intended to be contained in a filing system. Files or sets of files as well as their cover pages, which are not structured according to specific criteria, should not fall within the scope of this Regulation.
- 14) This Regulation does not address issues of protection of fundamental rights and freedoms or the free flow of data related to activities which fall outside the scope of Union law, such as activities concerning national security, taking into account Articles 3 to 6 of the Treaty on the Functioning of the European Union (...) nor does it cover the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.

- 14a) Regulation (EC) No 45/2001¹ applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Regulation (EC) No 45/2001 and other Union legal instruments applicable to such processing of personal data should be adapted to the principles and rules of this Regulation.
- 15) This Regulation should not apply to processing of personal data by a natural person in the course of a personal or household activity, and thus without a connection with a professional or commercial activity. Personal and household activities include social networking and on-line activity undertaken within the context of such personal and household activities. However, this Regulation should (...) apply to controllers or processors which provide the means for processing personal data for such personal or domestic activities.
- 16) The protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences, and, for these purposes, the maintenance of public order, or the execution of criminal penalties and the free movement of such data, is subject of a specific legal instrument at Union level. Therefore, this Regulation should not apply to the processing activities for those purposes. However, data processed by public authorities under this Regulation when used for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties should be governed by the more specific legal instrument at Union level (Directive XX/YYYY).

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

¹ OJ L 8, 12.1.2001, p. 1.

- 16a) While this Regulation applies also to the activities of courts and other judicial authorities, Union or Member State law could, (...), specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities. The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks. Supervision of such data processing operations may be entrusted to specific bodies within the judicial system of the Member State, which should in particular control compliance with the rules of this Regulation, promote the awareness of the judiciary of their obligations under this Regulation and deal with complaints in relation to such processing.
- 17) Directive 2000/31/EC does not apply to questions relating to information society services covered by this Regulation. That Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between Member States. Its application should not be affected by this Regulation. This Regulation should therefore be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

- 18) 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 may 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 the interest of public access to official documents with the right to the protection of personal data. **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**². **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.**
- 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.

² DK proposal.

- 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.

23) The principles of data protection should apply to any information concerning an identified or identifiable natural person. Data including pseudonymised data, which could be attributed to a natural person by the use of additional information, should be considered as information on an identifiable natural person. To determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by any other person to identify the individual directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the individual, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development. The principles of data protection should therefore not apply to anonymous information, that is information which does not relate to an identified or identifiable natural person or to data rendered anonymous in such a way that the data subject is not or no longer identifiable. This Regulation does therefore not concern the processing of such anonymous information, including for statistical and research purposes.

The principles of data protection should not apply to deceased persons, unless information on deceased persons is related to an identified or identifiable natural person³.

24) When using online services, individuals may be associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers. This may leave traces which, when combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them. Identification numbers, location data, online identifiers or other specific factors as such should not (...) be considered as personal data (...) if they do not identify an individual or make an individual identifiable⁴.

³ FR suggested this sentence be deleted.

⁴ DE reservation. ES, EE and IT also queried as regard the status of so-called identifiers. AT and SI thought the last sentence of the recital should be deleted. UK questioned whether so-called identifiers which were never used to trace back to a data subject should also be considered as personal data and hence subjected to the Regulation. It suggested stating that these can constitute personal data, but this will depend on the context. UK suggests deleting the words 'provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers' and 'received by the servers'. It also suggests deleting 'need not necessarily be considered as personal data in all circumstances' and replacing it by 'can constitute personal data, but this will depend on the context'. COM referred to the ECJ case law (Scarlett C-70/10) according to which IP addresses should be

- 25) Consent should be given unambiguously by any appropriate method enabling a freely-given, specific and informed indication of the data subject's wishes, either by a written, oral or other statement or by a clear affirmative action by the data subject signifying his or her agreement to personal data relating to him or her being processed. This could include ticking a box when visiting an Internet website or any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Where it is technically feasible and effective, the data subject's consent to processing may be given by using the appropriate settings of a browser or other application. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, unambiguous consent should be granted for all of the processing purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.
- 25a) Genetic data should be defined as personal data relating to the genetic characteristics of an individual which have been inherited or acquired as they result from an analysis of a biological sample from the individual in question, in particular by chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis or analysis of any other element enabling equivalent information to be obtained.
- 26) Personal data concerning health should include (...) data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health of the data subject; including information about the registration of the individual for the provision of health services (...); a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; (...) information derived from the testing or examination of a body part or bodily substance, including genetic data and biological samples; (...) or any information on for example a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as for example from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.

considered as persona data if they actually could lead to the identification of data subjects.
DE queried who would in practice be responsible for such metadata.

- 27) The main establishment of a controller in the Union should be the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union. In this case the latter should be considered as the main establishment. The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes (...) and means of processing through stable arrangements. This criterion should not depend on whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore not determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union and, if it has no central administration in the Union, the place where the main processing activities take place in the Union⁵. Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered as the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking.
- 28) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exercise a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented.
- 29) Children deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data. (...)⁶.

⁵ Obviously this recital may need to be amended in the context of future discussion on the one-stop-shop principle.

⁶ COM reservation on deletion of the reference to the UN Convention on the Rights of the Child.

- 30) Any processing of personal data should be lawful and fair. It should be transparent for the individuals that personal data concerning them are collected, used, consulted or otherwise processed and to which extent the data are processed or will be processed. The principle of transparency requires that any information and communication relating to the processing of those data should be easily accessible and easy to understand, and that clear and plain language is used. This concerns in particular the information of the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the individuals concerned and their right to get confirmation and communication of personal data being processed concerning them.

Individuals should be made aware on risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise his or her rights in relation to the processing. In particular, the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the collection of the data. The data should be adequate and relevant (...) for the purposes for which the data are processed; this requires in particular ensuring that the data collected are not excessive and that the period for which the data are stored is limited to a strict minimum. (...). Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or the use of personal data and the equipment used for the processing.

- 31) In order for processing to be lawful, personal data should be processed on the basis of the consent of the person concerned or some other legitimate legal basis laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. Whereas a legal basis does not necessarily require a legislative act adopted by a parliament⁷, it should be clear and precise and its application foreseeable for those subject to it as required by the case law of the Court of Justice of the European Union **and the European Court on Human Rights**⁸.
- 32) Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given the consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware that, and the extent to which, consent is given. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended; consent should not be regarded as freely-given if the data subject has no genuine and free choice and is unable to refuse or withdraw consent without detriment.
- 33) (...)
- 34) In order to safeguard that consent has been freely-given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller and this imbalance makes it unlikely that consent was given freely in all the circumstances of that specific situation. (...)
- 35) Processing should be lawful where it is necessary in the context of a contract or the intended entering into a contract.

⁷ This sentence does not mandate Member States to adopt such rules in ways other than by acts of parliament, but merely allows them to do so.

⁸ Further to SI suggestion.

- 35a) This Regulation provides for general rules on data protection. However in specific cases Member States are also empowered to lay down national rules on data protection. The Regulation does therefore not exclude Member State law that defines the circumstances of specific processing situations, including determining more precisely the conditions under which processing of personal data is lawful. National law may also provide for special processing conditions for specific sectors and for the processing of special categories of data. National law may thus provide for *specific rules on the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective labour agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.*
- 36) Where processing is carried out in compliance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority, the processing should have a (...) basis in Union law or in the national law of a Member State. (...). It should be also for Union or national law to determine the purpose of the processing. Furthermore, this (...) basis could specify the general conditions of the Regulation⁹ 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.

⁹ DK would prefer to delete "of the Regulation" and refer simply to the general conditions.

- 37) The processing of personal data should equally be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's life or that of another person.
- 38) The legitimate interests of a controller including of a controller to which the data may be disclosed may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding. This would need careful assessment including whether a data subject can expect at the time and in the context of the collection of the data that processing for this purpose may take place. In particular such assessment must take into account whether the data subject is a child, given that children deserve specific protection. The data subject should have the right to object to the processing, on grounds relating to their particular situation and free of charge. To ensure transparency, the controller should be obliged to explicitly inform the data subject on the legitimate interests pursued and on the right to object, and also be obliged to document these legitimate interests. Given that it is for Union or national law to provide (...) the (...) basis for public authorities to process data, this legal ground should not apply for the processing by public authorities in the exercise of their public duties.
- 39) The processing of data to the extent strictly necessary for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems, by public authorities, Computer Emergency Response Teams – CERTs, Computer Security Incident Response Teams – CSIRTs, providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller *concerned*. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping ‘denial of service’ attacks and damage to computer and electronic communication systems. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes can be regarded as carried out for a legitimate interest.¹⁰

¹⁰ UK thought that this recital should also contain a reference to the use of pseudonymous data.

- 40) The processing of personal data for other purposes should be only allowed where the processing is compatible with those purposes for which the data have been initially collected, in particular where the processing is necessary for archiving, 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.
- 41) Personal data which are, by their nature, particularly sensitive (...) in relation to fundamental rights and freedoms, deserve specific protection as the context of their processing may create important risks for the fundamental rights and freedoms¹¹. These data should also include personal data revealing racial or ethnic origin, whereby the use of the term ‘racial origin’ in this Regulation does not imply an acceptance by the European Union of theories which attempt to determine the existence of separate human races. Such data should not be processed, unless processing is allowed in specific cases set out in this Regulation. In addition to the specific requirements for such processing, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing such special categories of personal data should be explicitly be provided for where the data subject gives his or her explicit consent or in respect of specific needs, in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.

¹¹ BE proposal.

Member State and Union Law may provide that the general prohibition for processing such special categories of personal data in certain cases may not be lifted by the data subject's explicit consent¹².

- 42) Derogating from the prohibition on processing sensitive categories of data should also be allowed when provided for in Union or Member State¹³ law, and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where important grounds of public interest so justify, *such as processing data for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious (...) threats to health or ensuring high standards of quality and safety of health care and services and of medicinal products or medical devices or assessing public policies adopted in the field of health, also by producing quality and activity indicators*¹⁴. This may in particular be done for health purposes, including public health and social protection and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for archiving, historical, statistical and scientific (...) purposes.

A derogation should also allow processing of such data where necessary for the establishment, exercise or defence of legal claims, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure.

- 43) Moreover, the processing of personal data by official authorities for achieving aims, laid down in constitutional law or international public law, of officially recognised religious associations is carried out on grounds of public interest.

¹² DK proposal.

¹³ Further to DK proposal.

¹⁴ Previously in Article 81.

- 44) Where in the course of electoral activities, the operation of the democratic system requires in a Member State that political parties compile data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established.
- 45) If the data processed by a controller do not permit the controller to identify a natural person (...) the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. (...). However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights.
- 121) Member States law should reconcile the rules governing freedom of expression, including journalistic, 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 artistic or literary expression may be subject to derogations or exemptions from certain provisions of this Regulation in order 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.**¹⁵ 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. (...) ¹⁶

¹⁵ FR proposal.

¹⁶ PL suggested adding: 'Therefore, Member States should classify activities as "journalistic" for the purpose of the exemptions and derogations to be laid down under this Regulation if the object of these activities is the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them. They should not be limited to media undertakings and may be undertaken for profit-making or for non-profit making purposes'.

- 122) (...) Special categories of personal data which deserve higher protection, may only be processed for health-related purposes where necessary to achieve those purposes for the benefit of individuals and society as a whole, in particular in the context of the management of health-care services and ensuring continuity of health-care and cross-border healthcare or health security, monitoring and alert purposes or for archiving, historical, statistical or scientific purposes as well as for studies conducted in the public interest in the area of public health¹⁷. Therefore this Regulation should provide for harmonised conditions for the processing of special categories of personal data concerning health, in respect of specific needs, in particular where the processing of these data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy¹⁸ (...). Union or Member State law should provide for specific and suitable measures so as to protect the fundamental rights and the personal data of individuals. (...).
- 123) The processing of special categories personal data concerning health may be necessary for reasons of public interest in the areas of public health, without consent of the data subject. This processing is subject to for suitable and specific measures so as to protect the rights and freedoms of individuals. In that context, ‘public health’ should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work, meaning all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of personal data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers, insurance and banking companies¹⁹.
- 124) (...)²⁰.

¹⁷ Further to FR proposal.

¹⁸ UK preferred the term 'confidentiality', but this does not appear to be the correct term for professional secrecy imposed by legal or deontological rules.

¹⁹ The Presidency suggests to move recitals 122 and 123 to 42a and 42b.

²⁰ Moved to recital 35a

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 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 purpose²¹ (...). 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, restriction of processing and on the right to data portability (...). The conditions and safeguards in question may entail specific procedures for data subjects to exercise those rights if this is appropriate in 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)(...) 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. Union law or national 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.

²¹ This sentence may be deleted, as it is already covered by recital 39.

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 Communities²² provides further specifications on statistical confidentiality for European statistics.

125b) The importance of archives for the understanding of the history and culture of Europe²³ 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 States²³. 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, unless information on deceased persons impinges the interests of **other identified or identifiable individuals**²⁴.

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 (...) ²⁵ 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 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, (...).

²² OJ L 87, 31.3.2009, p. 164–173.

²³ OJ C 113, 13.5.2003, p. 2.

²⁴ ES and MT thought that it was repetitious to refer to the non-application to deceased persons (also *e.g.* in recital 126, end first paragraph). MT added that certain sensitive data of deceased could be interesting, for example it would be interesting for a child to know if a deceased parent had a certain illness. MT suggested to add text like "if it did not impinge the interests of other data subjects". Support from EE and SK to the MT suggestion. SK suggested alternatively drafting on the lines that data on deceased persons linked to living persons could be used.

²⁵ SE wanted to delete the reference to *main mission* because very few entities have as their main mission to acquire access to records, but it is something that they do, such a drafting would narrow down the scope. Support from DK, IE and EE.

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 subject²⁶. 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 treasures²⁷.

126) Where personal data are processed for scientific (...) purposes, this Regulation should also apply to that processing. (...) 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 measures²⁸.

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 person, unless information on deceased persons impinges the interests of **other identified or identifiable individuals**.

(...).

²⁶ CZ, DK, FI, HU, FR, MT, NL, PT, RO, SE, SI and UK scrutiny reservation.

²⁷ FR proposal.

²⁸ CZ, DK, FI, FR, HU, MT, NL, PT, RO, SE, SI and UK scrutiny reservation. PL suggested to add the following text somewhere in the recital " When data are being processed for historical or archival purposes, the data subject shall have the right to obtain completion of incomplete or out of date personal data by means of providing a supplementary statement."

- 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 secrecy²⁹.
- 128) This Regulation respects and does not prejudice the status under national law of churches and religious associations or communities in the 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 data³⁰.
2. This Regulation protects (...) fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

²⁹ CZ suggested adding a sentence: "This is without prejudice to existing Member State obligations to adopt professional secrecy where required by Union law". One should consider whether this recital would not be better placed among the recitals related to Chapter VI.

³⁰ DE scrutiny reservation: DE thought that it was difficult to determine the applicability of EU data protection rules to the public sector according to internal market implications of the data processing operations.

- 2a. (...) Member States may maintain or introduce national provisions to further specify the application of rules of this Regulation with regard to the processing of personal data **for compliance with a legal obligation or** for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or for other specific processing situations **as provided for in Article 6(1)(c) and (e)** by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing **including for other specific processing situations as provided for in Chapter IX**³¹.

[Each Member State shall notify to the Commission the text of the provisions referred to in this paragraph by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them].

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.^{32 33}

³¹ This option was supported by PT, FR, IE, PL, LV, RO. Another option for a minimum harmonisation clause for the public sector (*Member States may maintain or introduce more stringent national provisions ensuring a higher level of protection of the rights and freedoms of the data subject, than those provided for in this Regulation, with regard to the processing of personal data by public authorities for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*) was supported by DK, NL, SE, SI and HR. ES could support both options. DE and HU expressed a preference for combining both options.

³² DK, FR, NL, SI scrutiny reservation. FR thought that this paragraph, which was copied from the 1995 Data Protection Directive (1995 Directive 95/46), did not make sense in the context of a Regulation as this was directly applicable.

³³ EE, FI, SE, and SI thought that the relation to other fundamental rights, such as the freedom of the press, or the right to information or access to public documents should be explicitly safeguarded by the operative part of the text of the Regulation. This is now regulated in Articles 80 and 80a of the draft Regulation.

Article 2

Material scope

1. This Regulation applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system³⁴.
2. This Regulation does not apply to the processing of personal data:
 - (a) in the course of an activity which falls outside the scope of Union law (...);
 - (b) (...);
 - (c) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V the Treaty on European Union;
 - (d) by a natural person (...) in the course of (...) a personal or household activity;
 - (e) by competent public authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences and, for these purposes³⁵, safeguarding of public security³⁶, or the execution of criminal penalties.
3. (...).

³⁴ HU, supported by SI objected to the fact that data processing operations not covered by this phrase would be excluded from the scope of the Regulation and thought this was not compatible with the stated aim of a set of comprehensive EU data protection rules. HU therefore proposed to replace the second part by the following wording 'irrespective of the means by which personal data are processed'. COM argued that this was meant to exclude hand-written notes, but HU and SI thought that the means by which personal data were recorded should be immaterial.

³⁵ BE reservation on the terms 'for these purposes'.

³⁶ The text needs to be aligned with the suggested text in the Data Protection Directive for police and judicial cooperation.

CHAPTER II

PRINCIPLES³⁷

Article 5

Principles relating to personal data processing

1. Personal data must be:
 - (a) processed lawfully, fairly³⁸ and in a transparent manner in relation to the data subject;
 - (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; further processing of personal data for archiving, statistical, scientific or historical purposes shall not be considered incompatible with the initial purposes;
 - (c) adequate, relevant and not excessive in relation to the purposes for which they are processed (...)³⁹;
 - (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
 - (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed solely for archiving, statistical, scientific or historical purposes purposes **subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of data subject**⁴⁰;

³⁷ DE and SI scrutiny reservations; SE scrutiny reservation on Article 5.

³⁸ DE thought this concept should be detailed; COM pointed out this was already done in recital 30.

³⁹ COM reservation on the deletion of the data minimisation principle.

⁴⁰ IE proposal so as to cover all the safeguards required under the Regulation, including those in Chapter IV.

- (ee) processed in a manner that ensures appropriate security (...) of the personal data.
 - (f) (...) ⁴¹
2. The controller shall be responsible for compliance with paragraph 1 ⁴².

Article 6

Lawfulness of processing ⁴³

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 ⁴⁴ consent to the processing of their personal data for one or more specific purposes ⁴⁵;
 - (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 (...) ⁴⁶;

⁴¹ AT wondered whether a principle of digital autonomy should be added here.

⁴² It was previously proposed to add '*also in case of personal data being processed on its behalf by a processor*', but further to suggestion from LU and FR, this rule on liability may be dealt with in the context of Chapter VIII.

⁴³ DE, AT, PT, SI, SE and SK scrutiny reservation.

⁴⁴ 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.

⁴⁵ UK suggested reverting to the definition of consent in Article 2(h) of the 1995 Directive.

⁴⁶ BG and ES scrutiny reservation; UK preferred the wording of the 1995 Directive.

- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller^{47 48};
 - (f) processing is necessary for the purposes of the legitimate interests⁴⁹ pursued by the controller or by a controller to which the data are disclosed⁵⁰ except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This subparagraph shall not apply to processing carried out by public authorities in the exercise of their public duties^{51 52}.
2. Processing of personal data which is necessary for **archiving**, historical, statistical or scientific **purposes** shall be (...) subject to the conditions and safeguards referred to in Article 83⁵³.
 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.

⁴⁷ COM clarified that this was the main basis for data processing in the public sector. DE, DK, LT and UK asked what was meant by 'public interest' whether the application of this subparagraph was limited to the public sector or could also be relied upon by the private sector. FR also requested clarifications as to the reasons for departing from the text of the 1995 Directive. UK suggested reverting to the wording used in Article 7(e) of the 1995 Directive.

⁴⁸ Subparagraphs (d) and (e) might have to be inverted.

⁴⁹ FR scrutiny reservation.

⁵⁰ BG, CZ, DE, ES, HU, IT, NL, SE and UK asked to reinstate the words 'or by a third party' from the 1995 Directive. COM, supported by FR, thought that the use of the concept 'a controller' should allow covering most cases of a third party.

⁵¹ ES and FR scrutiny reservation. BE, DK, SI, PT and UK had suggested deleting the last sentence.

⁵² 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.

⁵³ Reinstated at the request of UK, FI and DE.

The purpose of the processing shall be determined in this legal basis or as regards the processing referred to in point (e) of paragraph 1, be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller⁵⁴. This legal basis may **further** specify inter alia the general conditions governing the lawfulness of data processing the controller, the type of data which are subject to the processing, the data subjects concerned; the entities to, and the purposes for which the data may be disclosed; the purpose limitation⁵⁵; 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 alia⁵⁶:

- (a) any link between the purposes for which the data have been collected and the purposes of the intended further processing;
- (b) the context in which the data have been collected;
- (c) the nature of the personal data;
- (d) the possible consequences of the intended further processing for data subjects;
- (e) the existence of appropriate safeguards⁵⁷.

⁵⁴ ES wanted start this sentence by stating: "While ensuring an equal or higher level of protection of the rights and freedoms of the data subject".

⁵⁵ FR thought the purpose limitation might be further clarified in a recital.

⁵⁶ DK, FI, NL, SI and SE stressed that the list should not be exhaustive. PT wanted to add consent by the data subject as an element.

⁵⁷ BG, DE, ES and PL reservation: safeguards in themselves do not make further processing compatible.

4. Where the purpose of further processing is incompatible with the one for which the personal data have been collected, the further processing must have a legal basis at least in one of the grounds referred to in points (a) to (e)⁵⁸ of paragraph 1⁵⁹ ⁶⁰ ⁶¹.
5. (...)

Article 7

Conditions for consent

1. Where Article 6(1)(a) applies the controller shall be able to demonstrate that unambiguous⁶² consent was given by the data subject.
- 1a. Where article 9(2)(a) applies, the controller shall be able to demonstrate that explicit consent was given by the data subject.
2. If the data subject's consent is to be given in the context of a written declaration which also concerns other matters, the request for consent must be presented in a manner which is clearly distinguishable (...) from the other matters.
3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal (...).
4. (...)

⁵⁸ FR and ES thought (f) should be added.

⁵⁹ DE, HU, IT, NL and PT scrutiny reservation. IT and PT thought paragraph 4 could be deleted.

⁶⁰ 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'.

⁶¹ 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.'

⁶² COM reservation related to the deletion of 'explicit' in the definition of consent.

Article 8

Conditions applicable to child's consent in relation to information society services⁶³

1. Where Article 6 (1)(a) applies, in relation to the offering of information society services directly to a child⁶⁴, the processing of personal data of a child below the age of 13 years⁶⁵ shall only be lawful if and to the extent that such consent is given or authorised by the child's parent or guardian.

The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the child's parent or guardian, taking into consideration available technology.

2. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child⁶⁶.
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 the methods to obtain verifiable consent referred to in paragraph 1(...)⁶⁷.

⁶³ CZ, DE, AT, SE, SI, PT and UK scrutiny reservation. CZ, SI and UK would prefer to see this Article deleted. UK thought children should not be singled out as the only category of vulnerable data subjects; NO proposes including a general provision stating that personal data relating to children cannot be processed in an irresponsible manner contrary to the child's best interest. Such a provision would give the supervisory authorities a possibility to intervene if for example adults publish personal data about children on the Internet in a manner which may prove to be problematic for the child. DE, supported by NO, opined this article could have been integrated into Article 7

⁶⁴ Several delegations (HU, FR, SE, PT) asked why the scope of this provision was restricted to the offering of information society services or wanted clarification (DE) whether it was restricted to marketing geared towards children. The Commission clarified that this provision was also intended to cover the use of social networks, insofar as this was not governed by contract law. DE thought that this should be clarified. HU and FR thought the phrase 'in relation to the offering of information society services directly to a child' should be deleted.

⁶⁵ Several delegations queried the expediency of setting the age of consent at 13 years: DE, FR, HU, LU, LV, RO and SI. DE, SI and RO proposed 14 years. COM indicated that this was based on an assessment of existing standards, in particular in the US relevant legislation (COPPA).

⁶⁶ DE, supported by SE, queried whether a Member State could adopt/maintain more stringent contract law. SI thought the reference should be worded more broadly to 'civil law', thus encompassing also personality rights.

4. The Commission may lay down standard forms for specific methods to obtain verifiable consent referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2)]⁶⁸.

Article 9

Processing of special categories of personal data⁶⁹

1. The processing of personal data, revealing racial or ethnic origin, political opinions, religious us or philosophical beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life (...) shall be prohibited.⁷⁰
2. Paragraph 1 shall not apply if one of the following applies:
 - (a) the data subject has given explicit consent to the processing of those personal data (...), except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; or

⁶⁷ ES, FR and SE scrutiny reservation.

⁶⁸ LU reservation. ES, FR, SE and UK suggested deleting paragraphs 3 and 4.

⁶⁹ SE, AT and NL scrutiny reservation. DE, supported by CZ, SE and UK, criticised on the concept of special categories of data, which does not cover all sensitive data processing operations. CZ, SE and UK pleaded in favour of a risk-based approach to sensitive data. There appeared to be no majority in favour of such 'open' approach. SK and RO thought the inclusion of biometric data should be considered. COM opined that the latter were not sensitive data as such. SK also pleaded in favour of the inclusion of national identifier.

⁷⁰ EE reservation; SE scrutiny reservation UK questioned the need for special categories of data. NL thought the list of data was open to discussion, as some sensitive data like those related to the suspicion of a criminal offence, were not included. SE thought the list was at the same time too broad and too strict. SI thought the list of the 1995 Data Protection Directive should be kept. FR and AT stated that the list of special categories in the Regulation and the Directive should be identical.

- (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller in the field of employment law **or a collective agreement**⁷¹ in so far as it is authorised by Union law or Member State law providing for adequate safeguards⁷²; or
- (c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent; or
- (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed outside that body without the consent of the data subjects; or
- (e) the processing relates to personal data which are manifestly made public⁷³ by the data subject; or
- (f) processing is necessary for the establishment, exercise or defence of legal claims⁷⁴; or

⁷¹ FI proposal; there are normally rights and obligations given to both parties when processing personal data. In the employment context rights and obligations derives from law and also from collective agreements which are based normally on legislation

⁷² DE queried whether this paragraph obliged Member States to adopt specific laws on data protection regarding labour law relations; COM assured that the paragraph merely referred to a possibility to do so.

⁷³ DE, FR, SE and SI raised questions regarding the exact interpretation of the concept of manifestly made public (e.g. whether this also encompassed data implicitly made public and whether the test was an objective or a subjective one).

⁷⁴ DE thought it should be clarified that also courts can process sensitive data.

- (g) processing is necessary for the performance of a task carried out for (...) ⁷⁵ reasons of public interest, on the basis of Union law or Member State law which shall ⁷⁶ provide for suitable **and specific** ⁷⁷ measures to safeguard the data subject's legitimate interests; or
- (h) processing (...) is necessary for the purposes of preventive or occupational medicine, **for the assessment of the working capacity of the employee** ⁷⁸, medical diagnosis, the provision of care or treatment or the management of health-care systems and services (...) **on the basis of Union law or Member State law** ⁷⁹ and subject to the conditions and safeguards referred to in paragraph 4 ⁸⁰;
- (ha) processing of genetic data is necessary for (...) medical purposes ⁸¹ and subject to the conditions and safeguards referred to in paragraph 4;

⁷⁵ The term 'important' was deleted further to remarks by CZ, ES, FR, NL and UK.

⁷⁶ NL suggested 'may'.

⁷⁷ NL proposal.

⁷⁸ FI proposal.

⁷⁹ COM, ES, IE, PL scrutiny reservation.

⁸⁰ DE and EE scrutiny reservation. DE and ES queried what happened in cases where obtaining consent was not possible (e.g. in case of contagious diseases; persons who were physically or mentally not able to provide consent); NL thought this should be further clarified in recital 42. BE queried what happened in the case of processing of health data by insurance companies. COM explained that this was covered by Article 9(2) (a), but SI was not convinced thereof.

⁸¹ Some delegations wanted to delete this point in its entirety: FR, SI. NL and UK wanted to include also criminal purposes (*'the performance of a task carried out by competent authorities on the basis of Union or Member State law for the purpose of prevention, investigation, detection or prosecution of criminal offences'*), but the Presidency thinks this is covered by the draft Directive. Should this not be the case, this point would indeed need to be amended.

(hb) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union law or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject data;

(i) processing is necessary for archiving (...), historical, statistical or scientific (...) purposes and subject to the conditions and safeguards referred to in Article 83 (...) [or is necessary for studies conducted in the public interest in the area of public health]⁸².

(j) (...) ⁸³

2a. (...) ⁸⁴

3. (...)

4. *Personal data referred to in paragraph 1 may on the basis of Union or Member State law be processed for the purposes referred to in points (h) **and (ha)** of paragraph 2 when (...) those data are processed by a (...) professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies to the obligation of professional secrecy⁸⁵, or by another person also subject to an (...) obligation of secrecy under Member State law or rules established by national competent bodies.*

⁸² Further to FR proposal. IE thought this was already covered by scientific research.

⁸³ NL and DE proposed adding "*insurance and reinsurance, in particular the conclusion and the performance of insurance contracts, the processing of statutory claims, the evaluation of risks, the establishment of tariffs, compliance with legal obligations and the combating of insurance fraud*". This was however viewed critically by AT, BE, EE, ES, FR, LU, PT, FI and UK.

⁸⁴ Moved to Article 9a.

⁸⁵ See clarification of the term professional secrecy in recital 122. PL would have preferred to refer to legal obligations, but some of the may not be laid down in (statutory) law. RO on the contrary thought it sufficient to refer to 'rules established by national competent bodies in the field of professional secrecy'.

4a. In case a transfer of personal data referred to Article 44(1)(f) involves personal data concerning health such transfer can take place only subject to the condition that those data will be processed by a health professional subject to the obligation of professional secrecy under the law of the third State concerned or rules established by national competent bodies to the obligation of professional secrecy, or by another person also subject to an (...) obligation of secrecy under the law of the third State concerned or rules established by national competent bodies⁸⁶.

Article 9a

Processing of data relating to criminal convictions and offences⁸⁷

*Processing of data relating to criminal convictions and offences or related security measures⁸⁸ may only be carried out either under the control of official authority (...)⁸⁹ **or when the processing is based on points (c) and (e) of Article 6(1)** and in so far as authorised by Union law or Member State law providing for adequate safeguards for the rights and freedoms of data subjects⁹⁰. A complete register of criminal convictions may be kept only under the control of official authority⁹¹.*

⁸⁶ COM, CZ and FI reservation; EE and UK scrutiny reservation. FR proposed also to add an obligation of pseudonymisation.

⁸⁷ The Presidency suggests putting this as a separate article, given the fact that Member States do not want to treat these data as sensitive data. EE reservation: under its constitution all criminal convictions are mandatorily public.

⁸⁸ Addition suggested so as to clarify that this is without prejudice to the use of other legal bases (such as consent). This may allay the concerns raised in this regard by NL and DK.

⁸⁹ This wording has been deleted as it merely repeated points c) and e) of Article 6(1).

⁹⁰ NL scrutiny reservation. UK queried the relationship between this paragraph and Article 2(2) (c). COM argued that the reference to civil proceedings in Article 8(5) of the 1995 Directive need not be included here, as those proceedings are as such not sensitive data. DE and SE were not convinced by this argument.

⁹¹ SE scrutiny reservation. UK reservation on last sentence.

Article 10

Processing not requiring identification

1. If the purposes for which a controller processes personal data do not require the identification of a data subject by the controller, the controller shall not be obliged to acquire (...) additional information nor to engage in additional processing in order to identify the data subject for the sole purpose of complying with (...) this Regulation.⁹².

2. Where, in such cases the controller is not in a position to identify the data subject, articles 15, 16, 17, 17a, 17b and 18 (...) do not apply except where the data subject, for the purpose of exercising his or her rights under these articles, provides additional information enabling his or her identification⁹³.

⁹² AT, DE, FR, HU and UK scrutiny reservation.

⁹³ DK, NL, SE and SI scrutiny reservation; COM reservation. BE thought this paragraph could also be moved to a recital.

SECTION 5 RESTRICTIONS

Article 21 ***Restrictions***⁹⁴

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 (...) ⁹⁵ Articles 12 to 20 and Article 32, when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard:
 - (aa) national security;
 - (ab) defence;
 - (a) public security;
 - (b) the prevention, investigation, detection and prosecution of criminal offences and, for these purposes, safeguarding public security⁹⁶, or the execution of criminal penalties;

⁹⁴ 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 assess creditworthiness (credit scoring), go beyond the Proposal for a Regulation. With an eye to Article 6(3), the Member States also need flexibility especially in the public sector or in the health sector when it comes to laying down and framing specific rules (esp. in regard to earmarking, the nature of the data and the recipient) and enacting stricter rules. DE and EE thought the derogations should distinguish between the private and the public sector.

⁹⁵ Further to the remarks by BE, DE, HU, FI, FR, LU, AT and PL the reference to Article 5 has been deleted, as the principles of Article 5 should never be derogated from. IE and UK opposed this; with IE citing the example of 'unfair' data collection by insurance companies which might be necessary to rebut false damage claims.

⁹⁶ This change in wording will need to be discussed, but the Presidency has suggested this change in order to align the text to the suggested text in the Data Protection Directive for police and judicial cooperation.

(c) other important objectives of general public interests of the Union or of a Member State⁹⁷, in particular an important⁹⁸ economic or financial interest of the Union or of a Member State, including, monetary, budgetary and taxation matters, **public health and social security**⁹⁹, 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 (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**¹⁰⁰.

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

⁹⁷ DE, IT scrutiny reservation as to the broad character of this exemption. SE thought it should be moved to a separate subparagraph.

⁹⁸ DK, FR and UK scrutiny reservation on the adjective 'important'.

⁹⁹ BE and FR suggestion.

¹⁰⁰ Further to DE proposal.

CHAPTER IX

PROVISIONS RELATING TO SPECIFIC DATA PROCESSING SITUATIONS

Article 80

Processing of personal data and freedom of expression and information¹⁰¹

1. The national law of the Member State shall (...) reconcile¹⁰² 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 purposes of paragraph 1**, Member States may¹⁰³ 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) (...) if they are necessary to¹⁰⁴ reconcile the right to the protection of personal data with the freedom of expression **and information**.

¹⁰¹ Reservation by BE; scrutiny reservation by DE, EE and SI. BE and UK thought that the balance between competing fundamental rights should be struck by the judiciary and not by the legislature. SE thought that it was important to keep a broad margin of appreciation for Member States.

¹⁰² HR, PL, PT and SI thought the term 'reconcile' was not very felicitous as both were fundamental rights.

¹⁰³ BE, DE, FR preferred 'shall'.

¹⁰⁴ BE, DE, FR preferred to replace the necessity test by 'in order to'

Article 80a

Processing of personal data and public access to official documents and reuse of public sector information¹⁰⁵

Personal data in official documents or in public sector information held by a public authority or a public body 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 and reuse of such official documents and public sector information¹⁰⁶ with the right to the protection of personal data pursuant to this Regulation.

*Article 80b*¹⁰⁷

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.

Article 81

Processing of personal data for health -related purposes

(...)¹⁰⁸

Article 81a

Processing of genetic data

(...)¹⁰⁹

¹⁰⁵ SK scrutiny reservation.

¹⁰⁶ Changes made further to FR proposal.

¹⁰⁷ DK, NL, PL, SK and SI scrutiny reservation.

¹⁰⁸ See Article 9(2)(h) and (4).

¹⁰⁹ See Article 9(2)(ha) and (4).

Article 82

Processing in the employment context¹¹⁰

1. Member States may **specify the application of rules of this Regulation 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 property¹¹¹** 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].

Article 82a

Processing for purposes of social protection

(...)

¹¹⁰ See recital 35a.

¹¹¹ FI proposal; this refers to normal practice in companies to protect their property or their customer's property as well as their employees (like alone working employees) and their customer's safety with camera surveillance.

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

1. Where personal data are processed for archiving, scientific, statistical 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, 18 and 19¹¹², insofar as such derogation is necessary for the fulfilment of the specific purposes.
2. The appropriate safeguards referred to in paragraph 1 shall ensure that technological and/or organisational protection measures pursuant to Chapter IV¹¹³ are applied to the personal data, in particular to make the data unintelligible to any person who is not authorised to access it, unless those measures prevent achieving the purpose of the processing and such purpose cannot be otherwise fulfilled. (...)

¹¹² NL and DK proposed adding a reference to Article 7. However, derogating from consent would require many more safeguards, if only to make sure that processing for scientific purposes is not performed regardless of an individual's wishes. FR suggested adding reference to Articles 23, 32, 33, 53 (1b)(d) and (e). PL suggested deleting the reference to Article 19

¹¹³ Further NL and IE comments.

Article 84

Obligations of secrecy^{114 115}

1. (...) Member States may adopt specific rules to set out the (...) ¹¹⁶ 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 national law or rules established by national competent bodies to an obligation of professional secrecy, other equivalent¹¹⁷ 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 ¹¹⁸.
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 them¹¹⁹.

Article 85

Existing data protection rules of churches and religious associations¹²⁰

(...).

¹¹⁴ UK preferred the term 'confidentiality', but this does not appear to be the correct term for professional secrecy imposed by legal or deontological rules.

¹¹⁵ DE, ES, IT, NL and UK scrutiny reservation. One should consider whether this articles would not be better linked to Article 53.

¹¹⁶ BE and DE suggestion to cover all powers set out in Article 53.

¹¹⁷ UK would prefer deleting 'equivalent'.

¹¹⁸ BE suggested adding a new paragraph: "The supervisory authority will consult the relevant independent professional body prior to taking a decision on data flows".

¹¹⁹ CZ reservation. RO remarked that a uniform approach should be established for this type of provision, which might need to be moved to Chapter XI on final provisions.

¹²⁰ NL and PT reservation.