Council of the
European Union

Brussels, 17 March 2016
(OR. en)

5419/16
ADD 1

Interinstitutional File:
2012/0011 (COD)

DATAPROTECT 2
JAI 38
MI 25
DIGIT 21
DAPIX 9
FREMP 4
CODEC 52

DRAFT STATEMENT OF THE COUNCIL'S REASONS

Subject:	Position of the Council at first reading with a view to the adoption of 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) - Draft Statement of the Council's reasons

I. INTRODUCTION

The Commission proposed on 25 January 2012 a comprehensive data protection reform comprising of:

- abovementioned proposal for a General Data Protection Regulation, which is intended to replace the 1995 Data Protection Directive (former first pillar);
- a proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, which is intended to replace the 2008 Data Protection Framework Decision (former third pillar).

The European Parliament adopted its Position at first reading on the proposed General Data Protection Regulation and Directive on 12th March 2014 (7427/14).

The Council agreed on a General Approach on 15 June 2015, thereby giving a negotiating mandate to the Presidency to enter into trilogues with the European Parliament (9565/15).

The European Parliament and the Council, at the level of respectively the Committee on Civil Liberties, Justice and Home Affairs and the Permanent Representatives Committee, confirmed on respectively 17 and 18 December 2015 agreement on the compromise text resulting from the negotiations in the trilogues.

At its meetings on 12 February 2016, the Council reached a Political agreement on the draft Regulation (5455/15). At its meeting on 21 April 2016, the Council adopted its Position at first reading which is fully in line with the compromise text on the Regulation agreed in the informal negotiations between the Council and the European Parliament.

The Economic and Social Committee submitted an opinion on the Regulation in 2012 (12388/12).

The European Data Protection Supervisor was consulted and delivered a first Opinion in 2012 (OJ C 192, 30.6.2012, p. 7) and a second opinion in 2015 (OJ C 301, 12.09.2015, p. 1-8).

The Fundamental Rights Agency submitted an opinion on 1 October 2012.

II. OBJECTIVE

The General Data Protection Regulation harmonises the data protection rules in the European Union. The objectives of the Regulation are to reinforce data protection rights of individuals, facilitate the free flow of personal data in the single market and reduce administrative burden.

III. ANALYSIS OF THE COUNCIL'S POSITION AT FIRST READING

A. General observations

In light of the objective of the European Council to secure agreement on the data protection reform by the end of 2015, the European Parliament and the Council have conducted informal negotiations to converge their positions. The text of the Council Position at first reading on the General Data Protection Regulation fully reflects the compromise reached between the two co-legislators, assisted by the European Commission.

The Council Position at first reading maintains the objectives of Directive 95/46/EC: protection of data protection rights and the free flow of data. At the same time, it seeks to adapt the data protection rules currently in force in light of the ever-increasing volume of personal data that is processed as a result of technological change and globalisation. With a view to making the Regulation future-proof, the data protection rules of the Council Position at first reading are technologically neutral.

In order to ensure a consistent level of protection for individuals throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market, the Council Position at first reading largely provides for a single set of rules that is directly applicable throughout the Union. This harmonisation will do away with the fragmentation stemming from the different laws of the Member States implementing Directive 95/46. Nevertheless, with a view to taking account of the requirements of specific data processing situations, including for the public sector, the Council Position at first reading allows Member States to further specify the application of the data protection rules laid down in the Regulation in their national law.

The protection of personal data is a fundamental right enshrined in Article 8(1) of the Charter of Fundamental rights of the European Union. Moreover, Article 16 of the Treaty on the Functioning of the European Union lays down that everyone has the right to the protection of personal data concerning him or her, whatever the nationality or residence, and that rules should be laid down for that purpose and for the purpose of the free movement of personal data. On that basis, the Council Position at first reading lays down the principles and rules on the protection of individuals with regard to the processing of their personal data.

In order to achieve the objectives of the Regulation, the Council Position at first reading strengthens the accountability of controllers (responsible for determining the purposes and the means of the processing of personal data) and processors (responsible for processing personal data on behalf of the controller) so as to promotea real data protection culture. Against that background, throughout the Regulation, a risk-based approach is introduced which allows for the modulation of the obligations of the controller and the processor according to the risk of the data processing they perform. Furthermore, codes of conduct and certification mechanisms contribute to compliance with the data protection rules. This approach prevents overly prescriptive rules and reduces administrative burden without reducing compliance. Moreover, the dissuasive character of the potential penalties that can be imposed creates incentives for controllers to comply with the Regulation.

The new data protection rules laid down in the Council Position at first reading also provide for strengthened and enforceable rights for citizens. This allows a better control of individuals over their personal data leading to more trust in online services at a cross-border scale which will boost the Digital Single Market. Children deserve specific protection as they may be less aware of the risks in relation to the processing of personal data, as well as of their rights.

Furthermore, the Council Position at first reading enhances the independence of supervisory authorities while harmonising their tasks and powers. The rules for cooperation between supervisory authorities and, where relevant, with the Commission in cross-border cases - the consistency mechanism - will contribute to a consistent application of the Regulation throughout the European Union. This will increase legal certainty and reduce administrative burden. Moreover, the one-stop-shop mechanism will provide for a single interlocutor for the controllers and processors in relation to their cross-border processing, including binding decisions in disputes by the newly established European Data Protection Board. As a result of this mechanism, the application of the Regulation will be more consistent. Moreover, it will provide more legal certainty and reduce administrative burden.

Finally, the Council Position at first reading lays down a comprehensive framework for the transfers of personal data from the European Union to recipients in third countries or in international organisations providing for new tools compared to Directive 95/46/EC.

B. Key issues

The Council and the European Parliament, assisted by the European Commission, in informal negotiations, converged their positions laid down in respectively the Council's general approach and in the Parliament's Position at first reading. The Council Position at first reading on the General Data Protection Regulation fully reflects the compromises found. The key issues of the Council Position at first reading are set out below.

1. Scope

1.1. Material scope of the Regulation and delineation with the law enforcement Directive

The Council Position at first reading provides that the General Data Protection 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 any structured set of personal data which are accessible according to specific criteria or are intended to form part of such structured set. The material scope of the General Data Protection Regulation and the scope of the Data Protection Directive in the field of law enforcement are mutually exclusive. It is specified that the Regulation does not apply to processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences, the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. This delineation enables law enforcement authorities, in particular the police, to apply, as a rule, the data protection regime of the Directive while ensuring a consistent and high level of protection of personal data for individuals that are subject to law enforcement operations.

1.2. EU institutions and bodies

With a view to ensuring uniform and consistent protection of data subjects with regard to the processing of their personal data, the Council Position at first reading indicates that the necessary adaptations of Regulation (EC) 45/2001 which applies to EU institutions, bodies, offices and agencies should follow after the adoption of the General Data Protection Regulation in order to allow it to be applicable at the same time as the General Data Protection Regulation.

1.3. Household exemption

In order to avoid setting rules that would create unnecessary burden for individuals, the Council Position at first reading provides that the Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity, thus having no connection with a professional or commercial activity.

1.4. Territorial scope

The Council Position at first reading creates a level playing field for controllers and processors in terms of territorial scope by covering all controllers and processors irrespective whether they are established in the Union or not.

First of all, the Regulation determines that data protection rules apply to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. Second, in order to ensure that individuals are not deprived of protection of their data, the Regulation applies to the processing of personal data of data subjects who are in the Union, even if a controller or processor is not established in the Union, but where its processing activities are related to the offering of goods or services to such data subjects in the Union, as well as the monitoring of their behaviour as far as their behaviour takes place within the European Union. In addition, determining the scope in such a way enhances legal certainty for controllers and data subjects (the individuals whose personal data are processed).

The Council Position at first reading also ensures that data subjects and supervisory authorities have a point of contact in the EU in case controllers or processors are not established in the Union but are covered by the scope of the Regulation: they must designate in writing a representative in the Union. In order to avoid unnecessary administrative burden, this obligation does not apply to processing that is unlikely to result in a risk for the rights and freedoms of individuals and to processing by a public authority or body of the third country.

2. Principles relating to personal data processing

The principles of data protection apply to any information concerning an identifiable or identified natural person, including information that can no longer be attributed to a specific data subject without the use of additional information as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable natural person (pseudonymisation). Compared to Directive 95/46, the Regulation largely provides for continuity with regard to the principles underlying processing of personal data. At the same time, the principle of "data minimisation" has been adjusted to take into account the digital reality and with a view to establishing a balance between protection of personal data, on the one hand, and possibilities for controllers to process data, on the other hand.

3. Lawfulness of processing

3.1. Conditions for lawfulness

With a view to providing legal certainty, the Council Position at first reading builds on the Directive 95/46 in specifying that processing of personal data is only lawful if at least one of the following conditions are fulfilled:

- consent of the data subject for one or more specific purposes;
- a contract;
- a legal obligation;
- protection of vital interests of the data subject or of another natural person;
- a task carried out in the public interest or in the exercise of official authority vested in the controller;
- the legitimate interests pursued by a controller or by a third party.

Two conditions deserve to be elaborated: consent and legitimate interests pursued by the controller or by a third party.

3.1.1. Consent

In order to allow processing of their personal data, a data subject may give his or her consent to the processing through a clear affirmative action establishing a freely given, specific, informed and unambiguous indication of his or her agreement to personal data relating to him or her being processed. Such consent covers all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent must be granted for all of the processing purposes. Moreover, the controller must be able to demonstrate that the data subject has given consent to the processing operation. Silence, pre-ticked boxes or inactivity therefore does not constitute consent. The framing of the concept of consent ensures continuity with the acquis that has developed with regard to the use of this concept on the basis of Directive 95/46/EC while contributing to a common understanding and application of consent throughout the European Union.

Furthermore, with a view to protecting the data subject's data protection rights, it is specified that, if the data subject has given his or her consent in the context of a written declaration which also concerns other matters, any part of that declaration which constitutes an infringement of the Regulation is not binding. Moreover, when assessing whether consent is freely given, utmost account must be taken whether, inter alia, the performance of a contract is made conditional on consent to processing that is not necessary for the performance of the contract.

Finally, in order to allow derogations from the general prohibition for processing special categories of personal data, the Council Position at first reading provides for a higher threshold than for other processing as the data subject must give his or her explicit consent to the processing of such sensitive personal data.

For children, the Council Position at first reading provides for a specific protective regime for consent by children in relation to the offering of information society services. The processing of personal data of a child below the maximum age of 16 years is lawful if it can reasonably be verified, taking into account available technology, that such consent is given or authorised by the holder of parental responsibility over the child. Member States that consider a lower age more appropriate are allowed to set a lower maximum age provided that it is not below 13 years.

3.1.2. Legitimate interest of the controller

Processing of personal data can be lawful if the processing is necessary for the purposes of the legitimate interests pursued by a controller or by a third party. However, such legitimate interests are not a sufficient ground for lawful processing 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.

The existence of a legitimate interest requires an assessment, including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for this purpose may take place. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest. Given that it is for the legislator to provide by law the legal basis for public authorities to process personal data, this does not apply to the processing of personal data by public authorities in the performance of their tasks.

3.2. Specific Member State rules adapting the application of the Regulation

The Council's Position at first reading allows Member States to maintain or introduce more specific provisions which adapt the application of the rules of the Regulation if personal data is processed for compliance with a legal obligation or 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. Derogations, specific requirements and other measures are further foreseen in relation to specific processing operations whereby Member States reconcile the right to protection of personal data with the right to freedom of expression and information, public access to public documents, processing of national identification numbers, processing in the employment context and processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

3.3. Further processing

The Council Position at first reading provides that processing for another purpose than the one for which the personal data has been originally collected is only lawful where that further processing is compatible with the purposes for which the personal data were originally processed. However, where the data subject has given his or her consent or where the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard, in particular, important objectives of general public interests, the controller is allowed to further process the personal data irrespective of the compatibility of the purposes. The rights of the data subject have been reinforced in the case of further processing, in particular as regards the right to information and the right to object to such further processing when it is not necessary for the performance of a task carried out for reasons of public interest.

In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data was originally collected, the controller must take into account *inter alia* any link between the original purposes and the purposes of the intended further processing, the context in which the personal data have been collected, in particular the reasonable expectations of the data subject based on his or her relationship with the controller as to the further use, the nature of the personal data, the consequences of the intended further processing for the data subject, and the existence of appropriate safeguards in both the original and the intended further processing operations.

3.4. Processing of special categories of personal data

Personal data which are, by their nature, particularly sensitive, deserve specific protection as the context of their processing may create important risks for the fundamental rights and freedoms of individuals. For that reason, as a rule, the Council Position at first reading maintains the approach of Directive 95/46 in prohibiting processing of special categories of personal data.

As a derogation to this rule, in certain, exhaustively listed situations, processing of sensitive data is allowed, for instance when the data subject has given explicit consent, when the processing is necessary for reasons of substantial public interest, or when the processing is necessary for other purposes, among others in the area of health.

Finally, the Council Position at first reading provides that Member States may introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or health data. However, these further conditions must not hamper the free flow of data within the Union.

4. Empowerment of data subjects

4.1. Introduction

The Council Position at first reading empowers data subjects by providing them with reinforced data protection rights and by putting obligations on controllers. The rights of the data subject encompass the right to information; to access to personal data; to rectification; to erasure of personal data, including a "right to be forgotten"; to restriction of processing; to data portability; to object; and not to be subject to a decision solely based on automated processing, including profiling. The rights that have been subject to important changes compared to Directive 95/46 are elaborated below.

Controllers are under an obligation to facilitate the exercise of data subjects' rights and to process personal data in line with the principle of transparency, in particular by providing information about the processing of personal data they carry out.

However, if the personal data processed by a controller do not permit the controller to identify a data subject, the data controller is not obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation.

Notwithstanding these rights of data subjects and these obligations of controllers, the Council Position at first reading maintains the approach of Directive 95/46 by allowing for restrictions of the general principles and the rights of the individual if such a restriction is based on Union or Member State law. Such restrictions must respect the essence of the fundamental rights and freedoms and be necessary and proportionate in a democratic society to safeguard certain public interests.

4.2. Transparency

In line with the principle of transparency, controllers must provide information and communication relating to processing of personal data in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed to a child. The information must be provided in writing, or by other means, where appropriate by electronic means.

The Council Position at first reading further lays down time limits for requests for information, communication or any other action by the controller, which must be exercised free of charge as a general rule. However, where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may charge a reasonable fee taking into account the administrative costs for providing the information or the communication or taking the action requested, or the controller may refuse to act on the request. In these cases, the controller bears the burden of demonstrating the manifestly unfounded or excessive character of the request.

4.3. Information and communication to be provided by the controller

With a view to finding a balance between, on the one hand, providing sufficient information to data subjects about the processing of their personal data, and, on the other hand, avoiding burdensome obligations for controllers, the Council Position at first reading sets out a two-step approach to ensure that data subjects are appropriately informed, both in cases where the personal data are collected from the data subject and in cases where the personal data have not been obtained from the data subject. In a first step, the controller is obliged to provide, at the time when personal data are obtained, to the data subject the information that is listed in the Regulation. In a second step, the controller must provide the additional information that is listed in the Regulation and that is necessary to ensure fair and efficient processing. Controllers shall also inform the data subjects when they intend to further process the personal data for a different purpose than the one for which the personal data were originally collected.

The controller is not obliged to provide the information listed in either the first or the second step where the data subject already possesses the information. Where the personal data were not obtained from the data subject, the controller shall not give any information to the data subject in case the recording or disclosure of the personal data to other parties is expressly laid down by law, or in case the provision of information to the data subject proves impossible or would involve disproportionate efforts.

Finally, controllers are obliged to communicate any rectification, erasure or restriction of processing to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves a disproportionate effort. Moreover; the controller must inform the data subject about those recipients if the data subject requests so.

4.4. Icons

The principles of transparent processing require that the data subject is informed of the existence of the processing and its purposes. Against that background, the Council Position at first reading lays down that information provided to the data subject may be accompanied with standardised icons. Controllers can decide on a voluntary basis whether the use of these standardised icons would be useful for the processing of personal data they carry out. The icons should present in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. The icons must be provided at the same time the information is given. Where the icons are presented electronically, they must be machine-readable. With a view to contributing to standardised use of icons in the EU, the Regulation empowers the Commission to adopt delegated acts determining the information that the icons should present, as well as the procedures for providing standardised icons. The European Data Protection Board must give an opinion on the icons proposed by the Commission. The possibility of adopting delegated acts does not prevent the European Data Protection Board from issuing guidelines, opinions and best practices on icons.

4.5. Right to access

The data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where such personal data are being processed, access to the information listed in the Regulation. In that light, the Regulation specifies that the controller must provide, free of charge, a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. The right to obtain a copy must not adversely affect the rights and freedoms of others.

4.6. Right to erasure ("right to be forgotten")

The Council Position at first reading entitles data subjects to have personal data concerning them erased where the processing of such data is not in compliance with the Regulation or with Union or Member State law to which the controller is subject.

The reference to the “right to be forgotten” acknowledges the need to adjust the right to erasure in particular in a digital context. Controllers that have made public the personal data that the data subject wants to be forgotten, must take reasonable steps, including technical measures, to inform controllers which are processing the personal data of the data subject's request to erase links to, or copies or replications of, such data, taking account of available technology and the cost of implementation. The European Data Protection Board may issue guidelines, recommendations and best practices on procedures for deleting links, copies or replications of personal data from publicly available communication services.

The right to erasure and the obligation for a controller to inform other controllers about the request to erasure do not apply to the extent that processing of personal data is necessary for purposes exhaustively listed in the Regulation, such as the right of freedom of expression and information.

4.7. Right to data portability

The Council Position at first reading sets out that, where processing of personal data is carried out by automated means, data subjects have the right to receive the personal data concerning them, which they provided to a controller in a structured, commonly used, machine-readable and interoperable format and to transmit this data to another controller. Moreover, it is specified that, where technically feasible, data subjects are entitled to have the personal data transmitted directly from one controller to another. This further strengthens the data subjects' control over their data. It also encourages competition amongst controllers.

However, this right to data portability does not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Furthermore, where, in a certain set of personal data, more than one data subject is concerned, the right of a data subject to receive the personal data is without prejudice to the rights and freedoms of others.

4.8. Right to object

In cases where personal data might lawfully be processed because processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or on grounds of the legitimate interests of a controller or a third party, the data subject is entitled to object to the processing of any personal data relating to his or her particular situation. In that case, the controller is no longer allowed to process the personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

Against this background, it is specified that where personal data are processed for direct marketing purposes, the data subject has the right to object at any time to the processing of personal data concerning him or her. This includes profiling to the extent that it is related to such direct marketing. Profiling is defined as any form of automated processing of personal data consisting of using those data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Where the data subject objects to the processing for direct marketing purposes, the personal data is no longer allowed to be processed for such purposes. Moreover, this right must be explicitly and clearly brought to the attention of the data subject at the latest at the time of the first communication of the personal data controller with the data subject.

Furthermore, the Council Position at first reading includes a reference to on-line do-not-track features by specifying that, in the context of the use of information society services, the data subject may exercise his or her right to object by automated means using technical specifications.

4.9. Automated individual decision-making, including profiling

The data subject has the right not to be subject to a decision based solely on automated processing which evaluates personal aspects relating to him or her and which produces legal effects concerning him or her or similarly significantly affects him or her. Examples are automatic refusal of an on-line credit application or e-recruiting practices without any human intervention. Such automated processing may include profiling. However, this right not to be subject to automated processing does not apply when it is necessary for:

- entering into, or for the performance of a contract between the data subject and a controller;

- when it is authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, such as fraud and tax evasion monitoring; or

- when it is based on the data subject's explicit consent.

- Except in the second case relating to processing authorised by Union or Member State law, the controller that performs processing by automated means must implement suitable safeguards for the rights and freedoms and legitimate interests of data subjects. These safeguards must at least include the right to obtain human intervention on the part of the controller and the possibility for the data subject to express his or her point of view and to contest the decision. Moreover, in order to ensure fair and transparent processing, controllers should use adequate mathematical and statistical procedures for the profiling and measures which minimise the potential risks for the interests of data subjects.

The data subject is further empowered because the controller is obliged to provide the data subject, when necessary to ensure fair and transparent processing, with information about the existence of automated decision-making, including profiling, and, at least in those cases, with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Finally, automated decision making and profiling based on special categories of personal data are only allowed under specific conditions, including the right of the data subject to object to such processing when these personal data are further processed for scientific and historical research purposes or statistical purposes, unless the processing is necessary for the performance of a task carried out in the public interest.

The European Data Protection Board may issue guidelines, recommendations and best practices for further specifying the criteria and conditions for decisions based on profiling.

5. Controller and Processor

5.1. Introduction

The Council Position at first reading establishes the legal framework for the responsibility and liability for any processing of personal data carried out by a controller or, on the controller's behalf, by a processor. In line with the principle of accountability, the controller is obliged to implement appropriate technical and organisational measures and be able to demonstrate the compliance of its processing operations with the Regulation. Against that background, the Regulation lays down rules relating to the responsibilities of the controller concerning impact assessments, keeping records of processing, data breaches, the designation of a Data Protection Officer and codes of conducts and certification mechanisms.

5.2. Impact assessments

The controller is responsible for the carrying out of a data protection impact assessment to evaluate when the processing is likely to result in a high risk for the rights and freedoms of individuals. The Council Position at first reading sets out the cases where a data protection impact assessment in particular is required, such as certain specific large-scale processing operations. In case such 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 must take place prior to the processing. The supervisory authority may then give advice to the controller and use any of its powers.

The European Data Protection Board may issue guidelines on processing operations that are likely 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 a potential risk.

5.3. Records of processing activities

In order to allow for *ex post* controls by the supervisory authority, the controller or, if any, the controller's representative, or the processor must keep records of processing activities under its responsibility, including on data breaches. With a view to reducing administrative burden, the obligation to record does not apply to enterprises or organisations employing less than 250 persons, unless the processing they carry out is likely to result in a risk for the rights and freedoms of data subjects, the processing is not occasional, or the processing includes sensitive data or data relating to criminal convictions and offences.

5.4. Data breaches

A personal data breach may result in physical, material or non-material damage to individuals such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorized reversal of pseudonymisation, damage to the reputation, loss of confidentiality of data protected by professional secrecy or any other economic or social disadvantage to the individual concerned. The Council Position at first reading provides that controllers must notify data breaches to supervisory authorities unless the data breach is unlikely to result in a risk for the rights and freedoms of individuals. They must also communicate to the data subjects concerned those breaches that are likely to present a high risk. Notification of the supervisory authorities will enable them to intervene, if necessary. Moreover, communication to the relevant data subject will make it possible for him or her to take precautionary measures.

With a view to reducing administrative burden, the Council Position at first reading applies different thresholds for notifications to the supervisory authority and communications to the relevant data subjects with a higher threshold for the communication than for the notification. Controllers are obliged, as soon as they become aware that a personal data breach has occurred, to notify without undue delay and, where feasible, not later than 72 hours after having become aware of it, the competent supervisory authority. However, controllers may refrain from notification if they are able to demonstrate that the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals. Besides some exceptions, controllers are obliged to communicate the data breach to the relevant data subjects, without undue delay, when the personal data breach is likely to result in a high risk to the rights and freedoms of those data subjects.

The European Data Protection Board may issue guidelines, recommendations and best practices for establishing the data breaches and determining the undue delay after the controller has become aware of the breach and for the particular circumstances in which a controller is required to notify the personal data breach, as well as for the circumstances in which a personal data breach is likely to result in a high risk for the rights and freedoms of the individuals.

5.5. Data Protection Officer

The purpose of designating a Data Protection Officer is it to improve compliance with the Regulation. Therefore, the Data Protection Officer must be a person with expert knowledge of data protection law and practices and must assist the controller or processor to monitor internal compliance with this Regulation. He or she may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract. A single Data Protection Officer may also be designated for a group of undertakings or where the controller or the processor is a public authority. The Council Position at first reading provides for the mandatory designation of a Data Protection Officer where:

- the processing is carried out by a public authority, except for courts or independent judicial authorities when acting in their judicial capacity,

- the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

- the core activities of the controller or the processor consist of processing on a large scale of sensitive data and data relating to criminal convictions and offences.

5.6. Codes of conduct and certification mechanisms

The Council Position at first reading incentivises the application of codes of conduct and promotes wider use of data protection certification mechanisms and data protection seals and marks. These initiatives contribute to compliance with the data protection rules while avoiding overly prescriptive rules and reducing costs for public authorities responsible for enforcement. Moreover, codes of conduct can take into account specific characteristics of processing carried out in certain sectors as well as the needs of micro, small and medium-sized enterprises. Certification mechanisms and data protection seals and marks for their part contribute to compliance with the Regulation as data subjects can easily assess the level of data protection of relevant products and services.

The Council Position at first reading comprises an elaborate set of rules with regard to codes of conduct and certification mechanisms, data protection seals and marks that give room for private initiative whilst protecting data protection standards through the involvement of supervisory authorities.

5.6.1. Codes of conduct

The supervisory authority can approve codes of conducts or amendments or extensions of such codes of conduct. Where the draft code of conduct relates to processing activities in several Member States, the competent supervisory authority must, before approval, submit a draft of amended or extended code to the European Data Protection Board for an opinion.

The Commission may adopt implementing acts for deciding that new codes of conduct and amendments or extensions to existing codes of conduct approved by the competent supervisory authority have general validity within the Union.

The European Data Protection Board should encourage the drawing up of codes of conduct. It must also collect all approved codes of conduct and amendments thereto in a register and make them publicly available through any appropriate means.

5.6.2. Certification mechanisms, data protection seals and marks

The Council Position at first reading sets out that each Member State must provide whether the certification bodies are accredited by the supervisory authority or by the National Accreditation Body. Accredited certification bodies can certify controllers and processors on the basis of the criteria approved by the competent supervisory authority or, in line with the consistency mechanism, the European Data Protection Board. In the latter case, the criteria approved by the European Data Protection Board may result in a common certification: the European Data Protection Seal. Certification is issued to a controller or processor for maximum 3 years with a possibility of renewal. The certification body must provide the supervisory authority with the reasons for granting or withdrawing the requested certification. Subsequently, the supervisory authority can reject or declare such a certification invalid.

The Commission is competent for adopting delegated acts for the purpose of specifying the requirements to be taken into account for the data protection certification mechanisms. The European Data Protection Board must give an opinion on these requirements. The Commission may also adopt implementing acts on 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.

Finally, the European Data Protection Board should encourage the establishment of data protection certification mechanisms and data protection seals and marks.

6. Transfer of personal data to third countries or international organisations

6.1. Introduction

Cross-border flows of personal data to and from countries outside the Union and international organisations are crucial in a context of global trade and cross-border digital economy. The level of protection guaranteed by the Union must not be undermined if personal data of EU citizens are transferred outside the Union.

As a general principle, any transfer of personal data to a third country or to an international organisation, may only take place if controllers and processors comply with the rules of the Regulation. The Council Position at first reading fully takes into account the case law of the Court of the European Union, including its ruling of 6 October 2015 in case C-362/14. The Council Position maintains the different ways for allowing cross-border transfers of personal data while strengthening guarantees that data protection rights are respected. These different ways to transfer personal data are adequacy decisions, appropriate safeguards and derogations.

The Council's Position at first reading clarifies that any ruling of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, in force between the requesting third country and the Union or a Member State. Moreover, the Council Position at first reading explicitly specifies that such international agreements are without prejudice to other grounds for cross-border transfers foreseen in the Regulation.

6.2. Adequacy decisions

International transfers may take place on the basis of a Commission adequacy decision that the third country, or a territory or one or more specific sectors within that third country, or the international organisation in question ensures a level of protection essentially equivalent to that guaranteed within the Union. Thus legal certainty and uniformity are provided throughout the Union.

The Commission may decide, having given notice and a complete justification to the third country or international organisation, to revoke an adequacy decision. The Commission adopts adequacy decisions and decisions to revoke such decisions as implementing acts. The implementing acts must provide for a mechanism of periodic review, at least every four years. The Commission must monitor developments in third countries and international organisations that could affect the functioning of the adequacy decisions. For the purposes of monitoring and of carrying out the periodic reviews, the Commission should take into consideration the views and findings of the European Parliament and the Council as well as other relevant bodies and sources. In the context of the evaluation and review of the Regulation, the Commission must also, at regular intervals, report to the Council and the European Parliament. Finally, the European Data Protection Board must provide the Commission with an opinion for the assessment of the adequacy of the level of protection in a third country or an international organisation, including for the assessment whether no longer an adequate protection level is ensured.

Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC remain in force until amended, replaced or repealed by a Commission Decision. In the same vein, authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC and decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC remain valid until amended, replaced or repealed, if necessary, by respectively that supervisory authority or by decision of the Commission. By ensuring continuity, the Council Position at first reading provides for legal certainty.

6.3. Appropriate safeguards

In addition to adequacy decisions, cross-border transfers can also take place if the controller or the processor has taken appropriate safeguards to compensate for the lack of data protection in the third country or international organisation. Such safeguards may consist of legally binding and enforceable instruments between public authorities or bodies, binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority. Controllers or processors in a third country may also provide appropriate safeguards for personal data transfers to third countries or international organisations. They can do so by an approved code of conduct together with binding and enforceable commitments to apply the appropriate safeguards via contractual or other legally binding instruments, including as regards data subjects' rights. They can also do so by a certification mechanism approved by the competent supervisory authority 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.

6.4. Derogations

In the absence of an adequacy decision or appropriate safeguards, a transfer or a set of transfers of personal data to a third country or an international organisation may take place on the basis of the derogations which are exhaustively listed in the Regulation. One of these derogations concerns the legitimate interests pursued by the controller in case the interests or rights and freedoms of the data subject do not override such interests. With a view to providing sufficient safeguards for cross-border transfers of personal data, the legitimate interests of the controller are strictly framed and may only be invoked as an *ultimum remedium*. With a view to ensuring a consistent application of the Regulation, the European Data Protection Board must, on its own initiative or at the request of the Commission, draw up and review guidelines, recommendations and best practices for the purpose of further specifying the criteria and requirements for data transfers in the absence of an adequacy decision or of appropriate safeguards.

7. Supervisory Authorities

7.1. Independence

In order to protect the fundamental rights and freedoms of individuals in relation to the processing of their personal data and to facilitate the free flow of personal data within the Union, each Member State must provide that one or more independent public authorities are responsible for monitoring the application of the Regulation on their territory. Each supervisory authority and its members must act with complete independence, including with integrity, in performing the tasks and exercising the powers entrusted to that supervisory authority and its members.

Each supervisory authority must contribute to the consistent application of the Regulation throughout the Union. For that purpose, the supervisory authorities must co-operate with each other and with the European Data Protection Board, as well as with the Commission. A consistent application of the Regulation is further ensured by laying down the competences of supervisory authorities and by defining the tasks and the investigative, corrective and the authorisation and advisory powers that the supervisory authorities must at least possess.

7.2. Professional secrecy

The Council Position at first reading sets out rules on professional secrecy for the supervisory authorities and its members. First of all, a member or members and the staff of each supervisory authority must, in accordance with Union or Member State law, be subject to a duty of professional secrecy, both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers. It is further specified that, during their term of office, this duty of professional secrecy applies in particular to reporting by individuals of infringements of the Regulation. Furthermore, the European Data Protection Board is tasked to issue guidelines, recommendations and best practices for establishing common procedures for reporting by individuals of infringements of the Regulation.

8. Cooperation and consistency

8.1. European Data Protection Board

The Council Position at first reading establishes the European Data Protection Board as body of the Union having legal personality with a view to ensuring a correct and consistent application of the Regulation. The interventions by the Board consist in particular of giving opinions, adopting binding decisions in the context of dispute resolution between supervisory authorities or issuing guidelines on any question covering the application of this Regulation in order to ensure the consistent enforcement of the Regulation.

The European Data Protection Board is composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives. The Commission has the right to participate in the activities and meetings of the European Data Protection Board without voting right. The discussions of the European Data Protection Board are confidential where the Board deems it necessary, as provided for in its rules of procedures.

In case the European Data Protection Board adopts a binding decision in the context of dispute resolution, the European Data Protection Supervisor has voting rights only on decisions which concern principles and rules applicable to the Union institutions, bodies, offices and agencies which correspond in substance to those of the Regulation.

8.2. Consistency mechanism

In cases of cross-border processing of personal data where more than one supervisory authority is involved, the consistency mechanism ensures that a single decision is taken which will be applicable throughout the European Union while taking into consideration the opinion of various concerned supervisory authorities. The consistency mechanism therefore enhances proximity between data subjects and the decision-making supervisory authority by involving the 'local' supervisory authorities in the decision-making process. Moreover, in case of disputes between supervisory authorities from different Member States, the newly created European Data Protection Board is competent to take binding decisions.

The rules of the consistency mechanism do not apply where the processing is carried out by public authorities or private bodies in the public interest. In such cases, the only supervisory authority competent is the supervisory authority of the Member State where the public authority or private body is established .

The Council's Position at first reading foresees that, in the context of the Commission's evaluation of the Regulation, the application of the cooperation and consistency mechanism will be examined.

9. Remedies, liabilities and penalties

The Council Position at first reading lays down an elaborate set of rules that enables data subjects several avenues for remedies, including to claim compensation in case of damage as a result of infringement of the Regulation.

9.1. Right to lodge a complaint and right to judicial remedy

The Council Position at first reading provides that every data subject has the right to lodge a complaint with a supervisory authority, if he or she considers that the processing of personal data relating to him or her does not comply with this Regulation. Moreover, each data subject has the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning him or her. He or she also has the right to an effective remedy in case the supervisory authority does not deal with the complaint or does not provide information on the progress or outcome of the complaint.

Each data subject further has the right to an effective judicial remedy if he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with the Regulation.

Proximity between data subject and national court is ensured as the data subject is entitled to have the decision of his or her data protection authority reviewed by his or her national court, irrespective in which Member State the controller or processor is established. Proceedings against a controller or a processor must be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

Finally, any natural or legal person has the right to bring an action for annulment of decisions of the European Data Protection Board before the Court of Justice of the European Union under the conditions provided for in Article 263 TFEU.

9.2. Representation of data subjects

A data subject has the right to mandate bodies, organisations or associations that fulfil specific criteria, such as working on a non-profit basis and being active in the field of data protection, to lodge the complaint on his or her behalf and to exercise the rights of judicial remedy on his or her behalf and to exercise the right to receive compensation on his or her behalf if provided for by Member State law. These specific criteria aim to avoid the development of a commercial claims culture in the field of data protection. In addition, Member States may provide that any such body, organisation or association, independently of a data subject's mandate, has in such Member State the right to lodge a complaint with the competent supervisory authority and to exercise the rights on judicial remedy, if it considers that the rights of a data subject have been infringed as a result of the processing of personal data that is not in compliance with the Regulation.

9.3. Suspension of proceedings

In order to avoid that the same subject matter as regards processing by the same controller or processor is scrutinised by different courts, any competent court other than the court first seized may suspend proceedings or, on the application of one of the parties, decline jurisdiction.

9.4. Right to compensation and liability

The Council Position at first reading provides that any data subject who has suffered material or non-material damage as a result of an infringement of the Regulation has the right to receive compensation from the controller or processor. With a view to giving data subjects the possibility to claim compensation in case of damage, while providing legal certainty to controllers and processors, the Regulation specifies their liabilities. Any controller involved in the processing is liable for the damage it has caused. A processor is liable only where it has not complied with obligations of the Regulation that are specifically directed to processors or has acted outside or contrary to lawful instructions of the controller. However, a controller or processor is exempted from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

Where more than one controller or processor or a controller and a processor are involved in the same processing and, where they are responsible for any damage caused by the processing, each controller or processor is held liable for the entire damage, in order to ensure effective compensation of the data subject. However, where a controller or processor has paid full compensation for the damage suffered, that controller or processor is entitled to claim back from the other controllers or processors involved in the same processing the part of the compensation that corresponds to their part of responsibility for the damage

9.5. Penalties

With the aim to ensure compliance with the Regulation, the Council Position at first reading provides that supervisory authorities can impose administrative fines. These fines must be effective, proportionate and dissuasive. Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State. Besides imposing administrative fines, supervisory authorities may also use other corrective powers such as warnings or reprimands. With a view to increasing harmonisation, the European Data Protection Board must draw up guidelines for supervisory authorities concerning the application of the supervisory authority's corrective powers and the fixing of administrative fines.

The Council Position at first reading contains a list of criteria for the supervisory authority when deciding whether to impose an administrative fine and, if so, what amount the fine should be. These criteria relate *inter alia* to the nature, gravity and duration or the intentional or negligent character of the infringement of the Regulation. The Regulation lists both the infringements and the corresponding maximum administrative fines. Within these maximum administrative fines, the supervisory authority must determine the appropriate amount depending on the circumstances of each individual infringement. With a view to providing legal certainty to controllers and processors and enhancing harmonisation of administrative fines within the Union, while keeping a margin of discretion for supervisory authorities, these infringements are subdivided in three categories. Infringements in the first category relating to the obligations of controllers and processors can be fined up to 10 000 000 EUR, or in case of an undertaking, up to 2% of the total worldwide annual turn-over of the preceding financial year, whichever is higher. The second category of infringements to the rights of the data subjects and the general principles has a ceiling of 20 000 000 EUR or 4% of the turnover. The third category of infringements concerns non-compliance with an order by the supervisory authority and also has a maximum fine of 20 000 000 EUR or 4% of turnover.

10. Specific data processing situations

10.1. Processing of personal data and freedom of expression and information

Member States must provide by law for the reconciliation of the right to the protection of personal data 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. With a view to ensuring transparency as regards reconciling these rights, each Member State is obliged to notify to the Commission the relevant provisions of its law and the amendments to those provisions, as well as new relevant provisions.

10.2. Processing in the employment context

Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context.

These rules must include suitable and specific measures to safeguard the data subject’s human dignity, legitimate interests and fundamental rights. Each Member State must notify to the Commission the relevant provisions of its law and the amendments to those provisions, as well as new relevant provisions.

10.3. Safeguards and derogations for processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

The Council Position at first reading establishes specific rules for processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.These rules aim at reconciling, on the one hand, the interest of the availability of personal data to maintain archives, to provide statistics and to do research, and, on the other hand, data protection rights.

Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is subject to appropriate safeguards for the rights and freedoms of the data subject. These safeguards provide that technical and organisational measures must be in place in particular in order to ensure that the principle of data minimisation is respected in case of processing for these specific purposes. These measures may include pseudonymisation, as long as these specific purposes can be fulfilled in this manner. Whenever these purposes can be fulfilled by further processing of personal data which does not permit or not any longer permit the identification of data subjects these purposes must be fulfilled in this manner. Subject to these safeguards and, in so far as such rights are likely to render impossible or seriously impair the achievement of processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, controllers are allowed to make derogations to some of the data protection rights contained in the Regulation provided that such derogations are necessary for the fulfilment of these specific purposes. These derogations are differentiated depending on the purpose of the processing. Notwithstanding the derogations already provided for in the Regulation as regards the right to information and the right to erasure (the 'right to be forgotten'), Union or Member State law may provide, under specific conditions and subject to appropriate safeguards, derogations from the right of access, the right to rectification, the right to restriction of processing, the notification obligation, the right to data portability and the right to object when processing personal data for archiving purposes in the public interest, as well as derogations from the right of access, the right to rectification, the right to restriction of processing and the right to object when processing personal data for scientific or historical research purposes or statistical purposes. Union or Member State law should provide for appropriate safeguards for such processing of personal data.

The Council Position at first reading also allows for a derogation to the prohibition to process sensitive personal data in case of processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Such derogation is allowed if the processing in question is based on Union or Member State law, which must be proportional to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

11. Previously concluded Agreements

The Council Position at first reading specifies that international agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to the entry into force of this Regulation, and which are in compliance with Union law applicable prior to the entry into force of this Regulation, remain in force until amended, replaced or revoked. This ensures legal certainty for controllers and prevents unnecessary administrative burden for Member States. It also takes into account that Member States depend on the cooperation of the third country or international organisation to amend existing agreements.

IV. CONCLUSION

The Council Position at first reading reflects the compromise reached in informal negotiations between the Council and the European Parliament, facilitated by the Commission. The Council invites the European Parliament to formally approve the Council Position at first reading without amendments, so that the new EU legislative framework for data protection can be established which will reinforce data protection rights while facilitating the flow of personal data in the digital market.