Basic information

2012/0011(COD) COD - Ordinary legislative procedure (ex-codecision procedure) Regulation	Procedure completed
Personal data protection: processing and free movement of data (General Data Protection Regulation) Repealing Directive 95/46/EC 1990/0287(COD) See also Directive 2002/58/EC 2000/0189(COD) See also 2012/0010(COD) See also 2023/0202(COD) **Subject** 1.20.09 Protection of privacy and data protection 2.80 Cooperation between administrations 3.45.05 Business policy, e-commerce, after-sales service, commercial distribution 4.60.06 Consumers' economic and legal interests	

Key players

European Parliament

Committee responsible	Rapporteur	Appointed
LIBE Civil Liberties, Justice and Home Affairs	ALBRECHT Jan Philipp (Verts/ALE)	12/04/2012
	Shadow rapporteur VOSS Axel (PPE) LAURISTIN Marju (S&D) IN 'T VELD Sophia (ALDE) KIRKHOPE Timothy (ECR) ERNST Cornelia (GUE/NGL) WINBERG Kristina (EFD)	

Former committee responsible	Former rapporteur	Appointed
LIBE Civil Liberties, Justice and Home Affairs	ALBRECHT Jan Philipp (Verts/ALE)	12/04/2012

Former committee for opinion	Former rapporteur for opinion	Appointed
ECON Economic and Monetary Affairs	The committee decided not to give an opinion.	
EMPL Employment and Social Affairs	HIRSCH Nadja (ALDE)	20/04/2012

ITRE Industry, Research and Energy	KELLY Seán (PPE)	14/03/2012
IMCO Internal Market and Consumer Protection	COMI Lara (PPE)	29/02/2012
JURI Legal Affairs	BOULLIER GALLO Marielle (PPE)	14/06/2012

Council of the European Union

Council configuration	Meetings	Date
Economic and Financial Affairs ECOFIN	3445	2016-02-12
Justice and Home Affairs (JHA)	3415	2015-10-09
Justice and Home Affairs (JHA)	3260	2013-10-07
Justice and Home Affairs (JHA)	3298	2014-03-03
Justice and Home Affairs (JHA)	3354	2014-12-04
Justice and Home Affairs (JHA)	3244	2013-06-06
Justice and Home Affairs (JHA)	3279	2013-12-06
Justice and Home Affairs (JHA)	3195	2012-10-25
Justice and Home Affairs (JHA)	3336	2014-10-10

European Commission

Commission DG	Commissioner
Justice and Consumers	REDING Viviane

European Economic and Social Committee

Key events

Date	Event	Reference	Summary
25/01/2012	Legislative proposal published	COM(2012)0011	Summary
16/02/2012	Committee referral announced in Parliament, 1st reading		
25/10/2012	Debate in Council		Summary
06/06/2013	Debate in Council		
07/10/2013	Debate in Council		Summary
21/10/2013	Vote in committee, 1st reading		
22/11/2013	Committee report tabled for plenary, 1st reading	A7-0402/2013	Summary
06/12/2013	Debate in Council		Summary
03/03/2014	Debate in Council		

11/03/2014	Debate in Parliament		
12/03/2014	Decision by Parliament, 1st reading	T7-0212/2014	Summary
12/03/2014	Results of vote in Parliament		
03/09/2014	Committee decision to open interinstitutional negotiations after 1st reading in Parliament		
10/10/2014	Debate in Council		Summary
04/12/2014	Debate in Council		Summary
17/12/2015	Approval in committee of the text agreed at 1st reading interinstitutional negotiations		
08/04/2016	Council position published	05419/1/2016	Summary
11/04/2016	Committee referral announced in Parliament, 2nd reading		
12/04/2016	Vote in committee, 2nd reading		
12/04/2016	Committee recommendation tabled for plenary, 2nd reading	A8-0139/2016	Summary
13/04/2016	Debate in Parliament		
14/04/2016	Decision by Parliament, 2nd reading	T8-0125/2016	Summary
14/04/2016	Results of vote in Parliament		
27/04/2016	Final act signed		
27/04/2016	End of procedure in Parliament		
04/05/2016	Final act published in Official Journal		

Technical information

Procedure reference	2012/0011(COD)
Procedure type	COD - Ordinary legislative procedure (ex-codecision procedure)
Procedure subtype	Legislation
Legislative instrument	Regulation
Amendments and repeals	Repealing Directive 95/46/EC 1990/0287(COD) See also Directive 2002/58/EC 2000/0189(COD) See also 2012/0010(COD) See also 2023/0202(COD)
Legal basis	Treaty on the Functioning of the European Union TFEU 114-p1 Treaty on the Functioning of the European Union TFEU 016-p2
Other legal basis	Rules of Procedure EP 165
Mandatory consultation of other institutions	European Economic and Social Committee
Stage reached in procedure	Procedure completed
Committee dossier	LIBE/8/03708

Documentation gateway

European Parliament

Document type	Committee	Reference	Date	Summary
Committee draft report		PE501.927	16/01/2013	
Committee opinion	IMCO	PE496.497	28/01/2013	
Committee opinion	ITRE	PE496.562	26/02/2013	
Committee opinion	EMPL	PE498.045	04/03/2013	
Amendments tabled in committee		PE504.340	04/03/2013	
Amendments tabled in committee		PE506.145	04/03/2013	
Amendments tabled in committee		PE506.146	04/03/2013	
Amendments tabled in committee		PE506.147	06/03/2013	
Amendments tabled in committee		PE506.164	06/03/2013	
Amendments tabled in committee		PE506.166	06/03/2013	
Amendments tabled in committee		PE506.168	06/03/2013	
Amendments tabled in committee		PE506.170	06/03/2013	
Amendments tabled in committee		PE506.173	08/03/2013	
Amendments tabled in committee		PE506.169	13/03/2013	
Committee opinion	JURI	PE494.710	25/03/2013	
Committee report tabled for plenary, 1st reading/single reading		A7-0402/2013	22/11/2013	Summary
Text adopted by Parliament, 1st reading/single reading		T7-0212/2014	12/03/2014	Summary
Committee draft report		PE580.501	04/04/2016	
Committee recommendation tabled for plenary, 2nd reading		A8-0139/2016	12/04/2016	Summary
Text adopted by Parliament, 2nd reading		T8-0125/2016	14/04/2016	Summary

Council of the EU

Document type	Reference	Date	Summary
Council position	05419/1/2016	08/04/2016	Summary
Draft final act	00017/2016/LEX	27/04/2016	

European Commission

Document type	Reference	Date	Summary
Legislative proposal	COM(2012)0011	25/01/2012	Summary
Document attached to the procedure	SEC(2012)0072	25/01/2012	
Document attached to the procedure	SEC(2012)0073	25/01/2012	
Commission response to text adopted in plenary	SP(2014)455	10/06/2014	
	COM(2016)0214		

Commission communication on Council's position		11/04/2016	Summary
Commission document (COM)	COM(2018)0043	24/01/2018	
Follow-up document	COM(2020)0264	24/06/2020	
Follow-up document	SWD(2020)0115	25/06/2020	
Follow-up document	COM(2024)0007	15/01/2024	
Follow-up document	SWD(2024)0003	15/01/2024	
Follow-up document	COM(2024)0357	25/07/2024	

National parliaments

Document type	Parliament /Chamber	Reference	Date	Summary
Contribution	PT_PARLIAMENT	COM(2012)0011	12/04/2012	
Contribution	FR_ASSEMBLY	COM(2012)0011	07/05/2012	
Contribution	CZ_SENATE	COM(2012)0011	30/05/2012	
Contribution	IT_SENATE	COM(2012)0011	02/07/2012	
Contribution	RO_CHAMBER	COM(2012)0011	20/10/2012	
Contribution	EE_PARLIAMENT	COM(2012)0011	02/10/2013	
Contribution	AT_BUNDESRAT	COM(2012)0011	27/10/2015	
Contribution	FR_SENATE	COM(2020)0264	10/12/2020	

Other institutions and bodies

Institution/body	Document type	Reference	Date	Summary
EDPS	Document attached to the procedure	N7-0083/2012 OJ C 192 30.06.2012, p. 0007	07/03/2012	Summary
EESC	Economic and Social Committee: opinion, report	CES1303/2012	23/05/2012	
EDPS	Document attached to the procedure	52015XX0912(01) OJ C 301 12.09.2015, p. 0001	27/07/2015	Summary

Additional information

Source	Document	Date
National parliaments	IPEX	

European Commission	EUR-Lex	
European Commission	EUR-Lex	

Final act
Corrigendum to final act 32016R0679R(02) OJ L 127 23.05.2018, p. 0002 Regulation 2016/0679 OJ L 119 04.05.2016, p. 0001 Summary

Personal data protection: processing and free movement of data (General Data Protection Regulation)

2012/0011(COD) - 25/01/2012 - Legislative proposal

PURPOSE: to protect individuals with regard to the processing of personal data and on the free movement of such data.

PROPOSED ACT: Regulation of the European Parliament and of the Council.

BACKGROUND: the centrepiece of existing EU legislation on personal data protection, Directive 95/46/EC, was adopted in 1995 with two objectives in mind: to protect the fundamental right to data protection and to guarantee the free flow of personal data between Member States. It was complemented by Framework Decision 2008/977/JHA as a general instrument at Union level for the protection of personal data in the areas of police co-operation and judicial co-operation in criminal matters.

The current legal framework remains sound as far as its objectives and principles are concerned, but it has not prevented fragmentation in the way personal data protection is implemented across the Union, legal uncertainty and a widespread public perception that there are significant risks associated notably with online activity.

This is why it is time to build a stronger and more coherent data protection framework in the EU, backed by strong enforcement that will allow the digital economy to develop across the internal market.

Personal data protection therefore plays a central role in the Digital Agenda for Europe, and more generally in the Europe 2020 Strategy.

- **Article 16(1) of Treaty on the Functioning of the European Union (TFEU)**, as introduced by the Lisbon Treaty, establishes the principle that everyone has the right to the protection of personal data concerning him or her.

- In 2010, the **European Council** invited the Commission to evaluate the functioning of EU instruments on data protection and to present, where necessary, further legislative and non-legislative initiatives.
- The Commission stressed in its Action Plan implementing the Stockholm Programme the need to ensure that the fundamental right to personal data protection is consistently applied in the context of all EU policies. In its Communication on "A comprehensive approach on personal data protection in the European Union", the Commission concluded that the EU needs a more comprehensive and coherent policy on the fundamental right to personal data protection.
- The European Parliament approved by its resolution of 6 July 2011 a report that supported the Commission's approach to reforming the data protection framework.

This proposal further details the approach for the **new legal framework** for the protection of personal data in the EU as presented in its Communication on this issue.

The legal framework consists of two legislative proposals:

- a **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), and
- a proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.

IMPACT ASSESSMENT: the impact assessment was based on the **three policy objectives** of improving the internal market dimension of data protection, making the exercise of data protection rights by individuals more effective and creating a comprehensive and coherent framework covering all areas of Union competence, including police co-operation and judicial co-operation in criminal matters.

Three policy options of different degrees of intervention were assessed:

- ***Option 1***: this option consisted of minimal legislative amendments and the use of interpretative Communications and policy support measures such as funding programmes and technical tools;
- ***Option 2***: this option comprised a set of legislative provisions addressing each of the issues identified in the analysis and
- ***Option 3***: this option was the centralisation of data protection at EU level through precise and detailed rules for all sectors and the establishment of an EU agency for monitoring and enforcement of the provisions.

The analysis of the overall impact led to the development of the preferred policy option which is based on the second option with some elements from the other two options and incorporated in the present proposal. According to the impact assessment, its implementation will lead *inter alia* to considerable improvements regarding legal certainty for data controllers and citizens, reduction of administrative burden, consistency of data protection enforcement in the Union, the effective possibility of individuals to exercise their data protection rights to the protection of personal data within the EU and the efficiency of data protection supervision and enforcement.

LEGAL BASIS: **Article 16(2) and Article 114(1)** of the Treaty on the Functioning of the European Union (TFEU).

CONTENT: the proposed Regulation lays down rules relating to the protection of individuals with regard to the processing of personal data and rules relating to the free movement of personal data. It protects the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data. It main provisions are as follows:

Principles: the proposal sets out the principles relating to personal data processing. Additional new elements are in particular the **transparency** principle, the clarification of the **data minimisation** principle and the establishment of a comprehensive responsibility and liability of the controller. It also sets out the criteria for lawful processing, which are further specified as regards the balance of interest criterion, and the compliance with legal obligations and public interest. It clarifies the conditions for consent to be valid as a legal ground for lawful processing and sets out further conditions for the lawfulness of the processing of personal data of children in relation to information society services offered directly to them.

Rights of the data subject: the proposal introduces the obligation on controllers to provide transparent and easily accessible and understandable information. It obliges the controller to provide procedures and mechanism for exercising the data subject's rights, including means for electronic requests, requiring response to the data subject's request within a defined deadline, and the motivation of refusals.

In addition, the proposal:

- further specifies the controller's information obligations towards the data subject, providing additional information to the data subject, including on the storage period, the right to lodge a complaint, in relation to international transfers and to the source from which the data are originating;
- provides the data subject's right of access to their personal data, such as to inform the data subjects of the storage period, and of the rights to rectification and to erasure and to lodge a complaint;
- sets out the data subject's right to rectification;
- provides the data **subject's right to be forgotten and to erasure**. It further elaborates and specifies the right of erasure provided for in Article 12 (b) of Directive 95/46/EC;
- introduces the data subject's right to **data portability**, i.e. to transfer data from one electronic processing system to and into another, without being prevented from doing so by the controller. As a precondition and in order to further improve access of individuals to their personal data, it provides the right to obtain from the controller those data in a structured and commonly used electronic format;
- provides for the data subject's **rights to object**;
- concerns the data subject's right not to be subject to a measure based on profiling.

General obligations: the proposal takes account of the debate on a "principle of accountability" and describes in detail the obligation of responsibility of the controller to comply with this Regulation and to demonstrate this compliance, including by way of adoption of internal policies and mechanisms for ensuring such compliance. It sets out the obligations of the controller arising from the principles of data protection by design and by default. It introduces for controllers and processors: (i) the obligation for controllers and processors to maintain documentation of the processing operations under their responsibility, instead of a general notification to the supervisory authority; (ii) the obligation to implement appropriate measures for the security of processing; (iii) an obligation to notify personal data breaches; (iv) the obligation of controllers and processors to carry out a data protection impact assessment prior to risky processing operations.

Data protection officer: the proposal introduces a **mandatory data protection officer** for the public sector, and, in the private sector, for large enterprises or where the core activities of the controller or processor consist of processing operations which require regular and systematic monitoring.

Transfer of personal data to third countries or international organisations: the proposal spells out, as a general principle, that the compliance with the obligations in that chapter are mandatory for any transfers of personal data to third countries or international organisations, including onward transfers. It sets out the criteria, conditions and procedures for the adoption of an adequacy decision by the Commission. The criteria which shall be taken into account for the Commission’s assessment of an **adequate or not adequate level of protection** include expressly the rule of law, judicial redress and independent supervision. The proposal requires for transfers to third countries, where no adequacy decision has been adopted by the Commission, to adduce appropriate safeguards, in particular standard data protection clauses, binding corporate rules and contractual clauses.

Independent supervisory authorities: the proposal obliges Member States to establish supervisory authorities and to enlarge the mission of the supervisory authorities to co-operation with each other and with the Commission. It clarifies the conditions for the independence of supervisory authorities, implementing case law by the Court of Justice of the European Union.

Co-operation and consistency: the proposal introduces explicit rules on mandatory mutual assistance, including consequences for non-compliance with the request of another supervisory authority. It introduces a consistency mechanism for ensuring unity of application in relation to processing operations which may concern data subjects in several Member States.

The proposal also establishes the European Data Protection Board, consisting of the heads of the supervisory authority of each Member State and of the European Data Protection Supervisor.

The European Data Protection Board replaces the Working Party on the Protection of Individuals with regard to the Processing of Personal Data set up under Article 29 of Directive 95/46/EC.

Remedies, liability and sanctions: the proposal provides: (i) for the right of any data subject to **lodge a complaint** with a supervisory authority, (ii) that the bodies, organisations or associations which may lodge a complaint on behalf of the data subject and also in case of a personal data breach **independently** of a data subject's complaint; (iii) for the right to a judicial remedy against a supervisory authority; (iv) the data subject may launch a court action for obliging the supervisory authority to act on a complaint; (v) the right to a judicial remedy against a controller or processor; (vi) for the introduction of common rules for court proceedings, including the rights of bodies, organisations or associations to represent data subjects before the courts, and the right of supervisory authorities to engage in legal proceedings; (vii) for the Member States to provide for the **right to compensation** and lay down rules on **penalties**, to sanction infringements of the Directive, and to ensure their implementation.

BUDGETARY IMPLICATIONS: the specific budgetary implications of the proposal relate to the tasks allocated to the European Data Protection Supervisor as specified in the legislative financial statements accompanying this proposal. These implications require reprogramming of Heading 5 of the Financial Perspective. The total appropriations are estimated at **EUR 24.339 million for 2014-2020**. The proposal has no implications on operational expenditure.

DELEGATED ACTS: this proposal contains provisions empowering the Commission to adopt delegated acts in accordance with Article 290 of the Treaty on the Functioning of the European Union.

Personal data protection: processing and free movement of data (General Data Protection Regulation)

2012/0011(COD) - 07/03/2012 - Document attached to the procedure

EDPS Opinion on the data protection reform package

On 25 January 2012, the Commission adopted a package for reforming the EU rules on data protection, which included:

- this proposal for a Regulation containing the general rules on data protection and
- a proposal for a Directive on data protection in the law enforcement sector.

The Regulation: the EDPS welcomes the proposed Regulation, as it constitutes a huge step forward for data protection in Europe. The proposed rules will strengthen the rights of individuals and make controllers more accountable for how they handle personal data. Furthermore, the role and powers of national supervisory authorities (alone and together) are effectively reinforced.

The EDPS is particularly pleased to see that the instrument of a regulation is proposed for the general rules on data protection. The proposed Regulation would be directly applicable in the Member States and would do away with many complexities and inconsistencies stemming from the different implementing laws of the Member States currently in place.

The Directive: the EDPS is, however, seriously disappointed with the proposed Directive for data protection in the law enforcement area. He **regrets that the Commission has chosen to regulate this matter in a self-standing legal instrument which provides for an inadequate level of protection,** and which is greatly inferior to the proposed Regulation.

A positive element of the proposed Directive is that it covers domestic processing, and thus has a wider scope than the current Framework Decision. However, this improvement only has added value if the Directive substantially increases the level of data protection in this area, which is not the case.

The **main weakness of the package as a whole** is that it does not remedy the lack of comprehensiveness of the EU data protection rules. It leaves many EU data protection instruments unaffected such as the data protection rules for the EU institutions and bodies, but also all specific instruments adopted in the area of police and judicial cooperation in criminal matters such as the Prüm Decision and the rules on Europol and Eurojust. Furthermore, the proposed instruments taken together do not fully address factual situations that fall under both policy areas, such as the use of PNR or telecommunication data for law enforcement purposes.

General comments on the proposed Regulation: the EDPS makes the following observations:

(1) One horizontal issue is the relationship between EU and national law. The proposed Regulation goes a long way in creating a single applicable law for data protection in the EU, however there is still more space for coexistence and interaction between EU law and national law than one might assume at first sight. The EDPS takes the view that the legislator should better acknowledge this.

(2) A second issue of general importance arises from the numerous provisions which empower the Commission to adopt delegated or implementing acts. The EDPS welcomes this approach in so far as it contributes to the consistent application of the Regulation, but has reservations about the extent to which essential legal provisions are left to delegated powers. Several of these empowerments should be reconsidered.

(3) On a detailed level, the EDPS points to the main positive elements of the proposed Regulation, which are:

- the clarification of the scope of application of the proposed Regulation;
- the enhanced transparency requirements towards the data subject and the reinforcement of the right to object;
- the general obligation for controllers to ensure and be able to demonstrate compliance with the provisions of the Regulation;
- the reinforcement of the position and role of national supervisory authorities;
- the main lines of the consistency mechanism.

The main negative elements of the proposed Regulation are:

- the new ground for exceptions to the purpose limitation principle;
- the possibilities for restricting basic principles and rights;
- the obligation for controllers to maintain documentation of all processing operations;
- the transfer of data to third countries by way of derogation;
- the role of the Commission in the consistency mechanism;
- the mandatory nature of imposing administrative sanctions.

General comments on the proposed Directive: as regards the Directive, the EDPS takes the view that the proposal, in many aspects, does not meet the requirement of a consistent and high level of data protection. It leaves all existing instruments in the area unaffected, and in many instances there is no justification whatsoever for departing from the provisions of the rules in the proposed Regulation.

The EDPS underlines that whilst the law enforcement area requires some specific rules, every departure from the general data protection rules should be duly justified based on a proper balance between the public interest in law enforcement and citizens' fundamental rights.

The EDPS is particularly concerned regarding:

- the lack of clarity in the drafting of the principle of purpose limitation;
- the absence of any obligation on competent authorities to be able to demonstrate compliance with the Directive;
- the weak conditions for transfers to third countries;
- the unduly limited powers of supervisory authorities.

The following recommendations on the whole reform process are made:

- announce publicly the time schedule on the second stage of the reform process as soon as possible;
- incorporate the rules for EU institutions and bodies in the proposed Regulation or at least have aligned rules in force when the proposed Regulation applies;
- present as soon as possible a proposal for common rules for the Common Foreign and Security Policy, based on Article 39 TEU.

The EDPS makes a **series of detailed recommendations** regarding amendments to provisions in both the draft regulation and the draft directive.

Personal data protection: processing and free movement of data (General Data Protection Regulation)

2012/0011(COD) - 14/04/2016 - Text adopted by Parliament, 2nd reading

The European Parliament adopted a legislative resolution on the Council position at first reading with a view to the adoption of a regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Following the recommendation for second reading by the Committee on Civil Liberties, Justice and Home Affairs, Parliament **approved the Council position at first reading**, without amendment.

Personal data protection: processing and free movement of data (General Data Protection Regulation)

2012/0011(COD) - 25/10/2012

The Council took note of the **state-of-play** on the proposal for a Regulation 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).

The **choice of legal instrument** was raised during the debate. Some delegations expressed their preference for a directive instead of a regulation since it allowed for more flexibility where this was needed. However, some other delegations preferred the choice of a regulation, as proposed by the Commission.

Ministers have already discussed this proposal at the informal ministerial meeting in July on the basis of three questions: the administrative burden, the need for special treatment for the public sector and the number of delegated acts.

The proposal is the subject of in-depth discussions by experts in the Working Party on Data Protection, which began under the Danish Presidency and will continue under the Irish Presidency.

Personal data protection: processing and free movement of data (General Data Protection Regulation)

2012/0011(COD) - 07/10/2013

The Council held an **in-depth discussion** on the present proposal.

To recall, the Commission presented in January 2012 a legislative package to modernise data protection rights. The package includes two legislative proposals:

- this draft regulation 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), and
- a draft directive on protecting personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities.

The “one-stop-shop” principle, together with the consistency mechanism, is one of the central pillars of the Commission proposal. According to this principle, when the processing of personal data takes place in more than one Member State, there should be **one single supervisory authority responsible for monitoring the activities of the controller** or processor throughout the Union and taking the related decisions. The proposal states that the authority acting as such a one-stop-shop should be the supervisory authority of the Member State in which the controller or processor has its main establishment.

The Council expressed its support for the principle that, in important transnational cases, the regulation should establish a "one-stop-shop" mechanism in order to arrive at a single supervisory decision, which should be fast, ensure consistent application, provide legal certainty and reduce administrative burden. This is an important factor to enhance the cost-efficiency of the data protection rules for international business, thus contributing to the growth of the digital economy.

The **discussion focused on how to arrive at such a single decision**. A majority of Member States indicated that further expert work should continue based on a model in which a single supervisory decision is taken by the “main establishment” supervisory authority, while the exclusive jurisdiction of that authority might be limited to the exercise of certain powers. Some Member States expressed their preference for the codecision mechanism, while others preferred to avoid taking any position on this point, at this stage.

The Council indicated that the experts should explore methods for enhancing the “proximity” between individuals and the decision-making supervisory authority by involving the local supervisory authorities in the decision-making process. This proximity is an important aspect of the protection of individual rights.

Another important element for increasing the consistency of the application of EU data protection rules will be to explore which powers and what role could be assigned to the European Data Protection Board (EDPB).

Personal data protection: processing and free movement of data (General Data Protection Regulation)

2012/0011(COD) - 22/11/2013 - Committee report tabled for plenary, 1st reading/single reading

The Committee on Civil Liberties, Justice and Home Affairs adopted the report by Jan Philipp Albrecht (Greens/EFA) on the 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).

The committee recommended that the Parliament’s position adopted in first reading following the ordinary legislative procedure should amend the Commission proposal. The key amendments are as follows:

Territorial Scope: the report provides that the Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, **whether the processing takes place in the Union or not**. It applies to a controller or processor not established in the Union, where the processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to data subjects in the Union.

Consent to processing: where processing is based on consent, the report confirms the controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes. It adds that:

- provisions on the data subject's consent which are partly in violation of the Regulation are fully void;
- it shall be as easy to withdraw consent as to give it. The data subject shall be informed by the controller if withdrawal of consent may result in the termination of the services provided or of the relationship with the controller;
- consent shall be purpose-limited and shall lose its validity when the purpose ceases to exist or as soon as the processing of personal data is no longer necessary for carrying out the purpose for which they were originally collected. The execution of a contract or the provision of a service shall not be made conditional on the consent to the processing of data that is not necessary for the execution of the contract or the provision of the service.

Right to erasure: the amendment in the report **reinforces the right to erasure of data** by allowing the data subject the right to obtain from third parties (to whom the data have been passed) the erasure of any links to, or copy or replication of that data. It also adds that the data subject has the right to erasure where:

- a court or regulatory authority based in the Union has ruled as final and absolute that the data concerned must be erased;
- the data has been unlawfully processed.

The controller and, where applicable, the third party shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary under certain specified grounds.

Notification requirement in the event of rectification and erasure: the controller shall communicate any rectification or erasure to each recipient to whom the data have been transferred, unless this proves impossible or involves a disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests this.

Standardised information policies: a new Article states that where personal data relating to a data subject are collected, the controller shall provide the data subject with certain particulars listed in the text before providing information required by the Regulation. Such particulars include whether personal data are collected beyond the minimum necessary for each specific purpose of the processing, and whether personal data are disseminated to commercial third parties.

The data controller would also be required to inform the person about various aspects of the data processing, such as the period of storage, the recipients of the personal data and the possible existence of profiling, as well as the data subject's rights of access, rectification and erasure of the data and right to lodge a complaint with a data protection authority.

Data portability: the committee deleted the Commission's provisions on data portability. The report provides that where personal data are processed by electronic means, the data subject shall have the right to obtain from the controller a copy of the provided personal data **in an electronic and interoperable format** which is commonly used and allows for further use by the data subject without hindrance from the controller from whom the personal data are withdrawn. Where technically feasible and available, the **data shall be transferred directly from controller to controller at the request of the data subject.**

Profiling: the report strengthens the **data subject's right to object to profiling**. The data subject shall be informed about the right to object to profiling in a highly visible manner. Profiling that has the effect of discriminating against individuals on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union membership, sexual orientation or gender identity, or that results in measures which have such effect, shall be prohibited. The controller shall implement **effective protection against possible discrimination** resulting from profiling.

The committee adds that profiling which leads to measures producing legal effects concerning the data subject shall **not be based solely or predominantly on automated processing** and shall include human assessment, including an explanation of the decision reached after such an assessment.

Transfers or disclosures not authorised by Union law: a new Article provides that no judgment of a court or tribunal and no decision of an administrative authority of a third country requiring a controller or processor to disclose personal data shall be recognised or be enforceable in any manner (without prejudice to international agreements). Where such a request is made of a controller, the latter must obtain prior authorisation for the transfer or disclosure by the supervisory authority. The data subjects must be informed.

A recital in the text adds that in cases where controllers or processors are confronted with **conflicting compliance requirements** between the jurisdiction of the Union on the one hand, and that of a third country on the other, the Commission should ensure that Union law takes precedence at all times. The Commission should provide guidance and assistance to the controller and processor, and it should seek to resolve the jurisdictional conflict with the third country in question.

Lead Authority: the report provides that where the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union takes place in more than one Member State, **one single supervisory authority should act as the single contact point and the lead authority responsible**. The lead authority, providing a one-stop shop, should be the supervisory authority of the Member State in which the

controller or processor has its main establishment or its representative. **The European Data Protection Board may designate the lead authority through the consistency mechanism in certain cases** on the request of a competent authority. The lead authority must consult other competent supervisory authorities in an endeavour to reach a consensus. However, it shall be the sole authority empowered to decide on measures intended to produce legal effects as regards the processing activities of the controller or processor for which it is responsible.

Data Protection Officers: the controller and the processor shall designate a data protection officer inter alia, where the processing is carried out by a legal person and relates to more than 5000 data subjects in any consecutive 12-month period.

Data protection officers shall be **bound by secrecy concerning the identity of data subjects** and concerning circumstances enabling data subjects to be identified, unless they are released from that obligation by the data subject. The committee changed the criterion from the number of employees a company has (the Commission suggested at least 250), to the number of data subjects. DPOs should be appointed for **at least four years** in the case of employees and two in that of external contractors. The Commission proposed two years in both cases.

Data protection officers should be in a position to perform their duties and tasks independently and **enjoy special protection against dismissal**. Final responsibility should stay with the management of an organisation. The data protection officer should be consulted prior to the design, procurement, development and setting-up of systems for the automated processing of personal data, in order to ensure the principles of privacy by design and privacy by default.

Administrative sanctions: additional provisions state that to anyone who does not comply with the obligations laid down in this Regulation, the supervisory authority shall impose at least one of the following sanctions:

- a warning in writing in cases of first and non-intentional non-compliance;
- regular periodic data protection audits;
- a fine up to 100 000 000 EUR or up to 5% of the annual worldwide turnover in case of an enterprise, whichever is higher (the Commission proposed up to EUR1 million or 2% of annual worldwide turnover). If the controller or the processor is in possession of a valid "European Data Protection Seal", a fine shall only be imposed in cases of intentional or negligent incompliance.

The administrative sanction shall take into account certain prescribed factors including the intentional or negligent character of the infringement, the degree of co-operation with the supervisory authority, in order to remedy the infringement and the level of damage, including non-pecuniary damage, suffered by the data subjects.

Personal data protection: processing and free movement of data (General Data Protection Regulation)

2012/0011(COD) - 12/03/2014 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 621 votes to 10 with 22 abstentions, a legislative resolution on the 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).

Parliament’s position in first reading following the ordinary legislative procedure amended the Commission proposal as follows:

Territorial Scope: Parliament stated that the Regulation applied **whether the processing takes place in the Union or not**. It applied to the processing of personal data of data subjects in the Union by a controller or processor not established in the Union, where the processing activities are related to linked.

Principles relating to personal data processing: these are: (i) lawfulness, fairness and transparency; (ii) purpose limitation; (iii) data minimization; (iv) accuracy; (v) storage minimization; (vi) integrity, meaning protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures; (vii) accountability.

Conditions of consent: the data subject should be informed in particular of the existence of the processing operation and its purposes, how long the data will be likely stored for each purpose, if the data are to be transferred to third parties or third countries.

Where processing is based on the data subject’s consent, Parliament confirmed that **the controller should have the burden of proving** that the data subject has given the consent to the processing operation.

Members added that:

- provisions on the data subject’s consent which are partly in violation of this Regulation are fully void;
- it should be as easy to withdraw consent as to give it. The data subject shall be informed by the controller if withdrawal of consent may result in the termination of the services provided or of the relationship with the controller.
- consent shall be purpose-limited and shall lose its validity when the purpose ceases to exist or as soon as the processing of personal data is no longer necessary for carrying out the purpose for which they were originally collected.

Information provided to children, parents and legal guardians in order to express consent, including about the controller’s collection and use of personal data, should be given in a clear language appropriate to the intended audience.

The following is prohibited: the processing of personal data, revealing race or ethnic origin, political opinions, religion or philosophical beliefs, sexual orientation or gender identity, trade-union membership and activities, and the processing of genetic or biometric data or data concerning health or sex life, administrative sanctions, judgments, criminal or suspected offences, convictions or related security measures.

General principles for data subject rights: Parliament proposed to strengthen, clarify, guarantee and where appropriate, codify these rights, which should be **clear and unambiguous**, and include:

- the provision of clear and easily understandable information regarding the processing of his or her personal data,
- the right of access, rectification and erasure of their data,
- the right to obtain data,
- the right to object to profiling, being any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person or to analyse or predict in particular that natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour;
- the right to lodge a complaint with the competent data protection authority and to bring legal proceedings as well as
- the right to compensation and damages resulting from an unlawful processing operation.

Such rights shall in general be exercised free of charge. The data controller shall respond to requests from the data subject within a reasonable period of time.

Standardised information policies: Parliament introduced a new Article stating that where personal data relating to a data subject are collected, the controller shall provide the data subject – **in an easily visible and clearly legible way and in a language easily understood -** with certain particulars listed in the text before providing information required by the Regulation.

Such particulars include: (i) whether personal data are collected beyond the minimum necessary for each specific purpose of the processing, and (ii) whether personal data are processed for purposes other than the purposes for which they were collected; (iii) whether personal data are disseminated to commercial third parties or sold or rented out; (iv) whether personal data are retained in encrypted form.

Right to erasure: Members reinforced this right by allowing the data subject to obtain from third parties the erasure of any links to, or copy or replication of, that data where one of the following grounds applies:

- a court or regulatory authority based in the Union has ruled as final and absolute that the data concerned must be erased;
- the data has been unlawfully processed.

Where the controller has made the personal data public without a justification, it shall take all reasonable steps to have the data erased, including by third parties. The controller shall inform the data subject, where possible, of the action taken by the relevant third parties.

Profiling: Parliament clarified that all persons have the **right to object to profiling**. The person concerned shall be informed about the right to object to profiling in a highly visible manner.

Profiling that has the effect of discriminating against individuals on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union membership, sexual orientation or gender identity, or that results in measures which have such effect, shall be prohibited. The controller shall implement effective protection against possible discrimination resulting from profiling.

Parliament added that profiling which leads to measures producing legal effects concerning the data subject shall **not be based solely or predominantly on automated processing** and **shall include human assessment**, including an explanation of the decision reached after such an assessment.

Security of processing: such a security policy shall include the ability: (i) to ensure that the integrity of the personal data is validated; (ii) to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data; (iii) to restore the availability and access to data in a timely manner in the event of a physical or technical incident.

Transfers or disclosures not authorised by Union law: a new Article provides that no judgment of a court or tribunal and no decision of an administrative authority of a third country requiring a controller or processor to disclose personal data shall be recognised or be enforceable in any manner (without prejudice to international agreements).

Lead authority: where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, Parliament proposed that the supervisory authority of the main establishment of the controller or processor shall act as the lead authority responsible for the supervision of the processing activities of the controller or the processor in all Member States.

Administrative sanctions: to anyone who does not comply with the obligations laid down in this Regulation, the supervisory authority shall impose at least one of the following sanctions:

- a warning in writing in cases of first and non-intentional non-compliance;
- regular periodic data protection audits;
- a fine **up to 100 000 000 EUR or up to 5% of the annual worldwide turnover** in case of an enterprise, whichever is higher.

If the controller or the processor is in possession of a valid "European Data Protection Seal", a fine shall only be imposed in cases of intentional or negligent incompliance.

Personal data protection: processing and free movement of data (General Data Protection Regulation)

2012/0011(COD) - 06/12/2013

The Council held an in-depth **discussion** on the proposal for a regulation setting out a general EU framework for data protection.

The discussion focused on the **one-stop-shop mechanism** in order to arrive at a single supervisory decision and related questions on **judicial review and judicial redress**.

The Council also indicated that the experts should explore methods for **enhancing the "proximity" between individuals and the decision-making supervisory authority** by involving the local supervisory authorities in the decision-making process.

However, during the discussions at expert level it was established that there are limits to guaranteeing proximity for data subjects while at the same time guaranteeing one-stop-shop supervision for businesses operating in the internal market. The need to reconcile these two important goals was the core issue in the debate.

The Presidency concluded that:

- there are different opinions as to whether the supervisory authority of the main establishment should be given limited exclusive powers to adopt corrective measures and that work should continue at technical level;
- it is important that the supervisory authorities cooperate in the enforcement of data protection rules;
- further work at technical level should include investigating the possibility of providing the European Data Protection Board in some cases with the power to adopt binding decisions regarding corrective measures.

Delegations are invited to indicate whether they agree that the main establishment authority, acting in close cooperation with local authorities, should, in addition to some exclusive authorisation powers, also be given certain exclusive powers to adopt corrective measures.

In case there would not be sufficient support for giving certain exclusive powers to adopt corrective measures to the main establishment authority, to indicate whether they think the power to decide on corrective measures should remain in the hands of the 'local' supervisory authorities in all cases or whether they could accept that in certain serious transnational cases the European Data Protection Board be given the power to adopt binding corrective measures.

Personal data protection: processing and free movement of data (General Data Protection Regulation)

2012/0011(COD) - 11/04/2016 - Commission communication on Council's position

The Commission **supports the political agreement** reached between the European Parliament and the Council in informal trilogues on 15 December 2015, since the agreement is in keeping with the objectives of the Commission proposal.

The proposal for a regulation focuses on reinforcing individuals' rights, strengthening the

EU internal market, ensuring stronger enforcement of the rules, streamlining international transfers of personal data and setting global data protection standards. The new rules provide for the following:

- **easier access to one's data:** individuals will have more information on how their data is processed in a clear and understandable way;
- **a "right to be forgotten":** when an individual no longer wants her/his data to be processed, and provided that there are no legitimate grounds for retaining it, the data will be deleted;
- **the right to know when one's data has been hacked:** companies must notify the supervisory authority of data breaches which put individuals at risk and communicate to the data subject all high risk breaches as soon as possible so that users can take appropriate measures;
- **a right to data portability:** this will make it easier for individuals to transmit personal data between service providers.

The proposed regulation also supports the digital single market to realise its potential through:

- **one continent, one law principle**;
- a **'one-stop-shop'** for businesses;
- a **level playing field:** companies based outside of Europe will have to apply the same rules when they offer goods or services on the EU market;
- **technological neutrality:** the regulation enables innovation to continue to thrive under the new rules.

The Commission notes that the agreement:

- maintains the nature of the legal instrument as proposed by the Commission, namely a **regulation** as opposed to a directive;
- ensures the **necessary level of harmonisation** while leaving room of maneouvre for Member States as regards the specifications of the data protection rules for the public sector;
- confirms the Commission approach as regards the **territorial scope** of the regulation which will also apply to controllers or processors established in a third country if they offer goods or services or monitor the behaviour of data subjects in the Union;
- strengthens the principles of **data processing** (e.g. data minimisation) and the rights of data subjects by enshrining a right to be forgotten and a right to portability and by further developing existing rights such as the right to information or the right of access;
- preserves and further develops the **risk-based approach**, which requires that controllers and, in some cases the processors, take into account the nature, scope, context and purposes of processing and the risks of varying likelihood and severity for the rights and freedoms of the data subject of such processing;
- provides that **"one-stop-shop"** mechanism is legally and institutionally sound, and maintains the key simplification element of having a single decision across the EU and a single interlocutor for business and for the individual;
- further clarifies and specifies the rules on **international transfers**;
- empowers supervisory authorities to impose **financial sanctions** for infringements of the Regulation, going up to 2 - 4% of the global annual turnover of an undertaking.

However, the Council position, contrary to the Commission proposal, **does not consider the regulation as a development of the Schengen *acquis***. Therefore, the Commission considers that a statement in this regard is necessary. In that statement, the Commission considers, in particular, that as far as visas, border control and return are concerned, the general data protection regulation constitutes a development of the Schengen acquis for the four States associated with the implementation, application and development of said acquis.

Personal data protection: processing and free movement of data (General Data Protection Regulation)

2012/0011(COD) - 12/04/2016 - Committee recommendation tabled for plenary, 2nd reading

The Committee on Civil Liberties, Justice and Home Affairs adopted the recommendation for second reading contained in the report by Jan Philipp ALBRECHT (Greens/EFA, DE) on the Council position at first reading with a view to the adoption of a regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

The committee recommended that Parliament approve the Council position in first reading without amendment.

To recall, the proposed regulation establishes rules regarding the protection of individuals with regard to the processing of personal data and rules on the free flow of such data. It will replace the 1995 Directive on data protection.

Personal data protection: processing and free movement of data (General Data Protection Regulation)

2012/0011(COD) - 27/04/2016 - Final act

PURPOSE: to modernise the existing rules on data protection in order to ensure a high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union (reform of data protection).

LEGISLATIVE ACT: Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

CONTENT: the new Regulation **establishes rules on the protection of natural persons with regard to the processing of personal data and on the free movement of such data**. It protects the fundamental rights and freedoms of natural persons, and particularly their right to protection of their personal data. The reform of data protection also includes a Directive on protection of data processed for the purpose of law enforcement (intended to replace the 2008 Framework Decision on data protection.)

The main points are as follows:

Scope: the Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. It applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, **regardless of whether the processing takes place in the Union or not**.

Principles relating to processing of personal data: personal data shall be:

- **processed lawfully, fairly and in a transparent manner** in relation to the data subject;
- **collected for specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes;
- **adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed;
- **kept** in a form permitting identification of the person concerned for a period that does not exceed what is necessary for the purposes of processing;
- processed in a manner that ensures **appropriate security** of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Lawfulness of processing: processing shall be lawful only if:

- the data subject has clearly and explicitly given consent to the processing;
- **processing is necessary** for: (i) the performance of a contract; (ii) compliance with a legal obligation; (iii) protecting the vital interests of the data subject or of another natural person; (iv) the performance of a task carried out in the public interest; (v) the purposes of the legitimate interests pursued by the controller or by a third party.

A specific protective regime is provided for consent by **children** in relation to the offering of information society services: if a **child below the age of 16 years** wishes to use online services, the service provider must verify that those with parental responsibility over the child have given their consent. Member States may lower this age limit, but it may not be below 13 years.

In principle, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. The data may, however, be processed under certain conditions set out in the Regulation.

Rights of the data subject: the Regulation sets out stronger rights in respect of data protection and strengthens the accountability of controllers. The rights of the data subject include:

- **the right to information:** this information must be concise, transparent, intelligible and easily accessible form, in particular for any information addressed specifically to a child. Natural persons must be informed about the policy in force with respect to data protection, in clear and simple terms; this may also be done through standardised icons;
- **the right of access to personal data**, i.e. 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 concerning, e.g. the purposes of the processing for which the personal data are intended, data categories, the recipients of the personal data, and where possible, the period for which the personal data will be stored;
- **the right of rectification** of incorrect data;
- **the right to erasure** to erasure of personal data, including the "**right to be forgotten**";
- **the right to restriction of processing**;
- **the right to data portability**, facilitating the transfer of personal data from one service provider, such as a social network, to another;
- **the right to object** and the right not be the subject of automated decision-making, including **profiling**. Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing.

These rights may be restricted where such restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to **safeguard national security, defence or public security**.

Responsibility of the controller or processor: the Regulation establishes the legal framework on the responsibility and liability for any processing of personal data carried out by a controller or, on the controller's behalf, by a processor. 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.

Data security: in order to maintain security and to prevent processing in infringement of the Regulation, the controller or processor should evaluate the risks inherent in the processing and implement **measures** to mitigate those risks, such as **encryption**. Those measures should ensure an appropriate level of security, including confidentiality.

The controller should **communicate** to the data subject a personal **data breach**, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. The controller should also notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than **72 hours** after having become aware of it.

Data protection officer: the controller and the processor shall designate a data protection officer in any case where a public authority or body carries out the processing. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under the Regulation.

Transfers of personal data outside the EU: as a general principle any transfer of personal data to a third country or to an international organisation may only take place if the controller and processor **comply with the rules** under the Regulation.

The Commission will decide, through implementing acts, that the third country or an international organisation ensures an adequate level of protection. The implementing act shall provide for a mechanism for a periodic review, at least every four years.

Supervision: to increase legal certainty and reduce administrative burden, in cross-border cases involving several national supervisory authorities, a **consistency mechanism is established**. The mechanism allows an enterprise active in several Member States to deal only with the data protection authority in the Member State in which it has its main establishment. The mechanism also provides for a single decision applicable to the whole EU in case of disputes.

Redress, responsibility and penalties: the Regulation sets out a detailed set of rules to allow persons to **claim judicial redress or compensation in case of damage** following a breach of the Regulation.

The Regulation provides that non-compliance with an order by the supervisory authority shall be subject to administrative fines up to **EUR 20 000 000, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover** of the preceding financial year, whichever is higher.

ENTRY INTO FORCE: 24.5.2016.

APPLICATION: from 25.5.2018.

DELEGATED ACTS: the Commission may adopt delegated acts, particularly in respect of criteria and requirements for certification mechanisms, information to be presented by standardised icons and procedures for providing such icons. The power to adopt such acts is conferred on the Commission for **an indeterminate period from 24 May 2016**. The European Parliament or the Council may raise objections to a delegated act within **three months** of the date of notification (this may be extended by three months.) If Parliament or Council raise objections, the delegated act will not come into force.

Personal data protection: processing and free movement of data (General Data Protection Regulation)

2012/0011(COD) - 27/07/2015 - Document attached to the procedure

European Data Protection Supervisor (EDPS) recommendations on the EU's options for data protection reform.

On 24 June 2015, the European Parliament, the Council and the European Commission entered co-decision negotiations on the proposed General Data Protection Regulation (GDPR), a procedure known as an informal 'trilogue'. The three institutions are committed to dealing with the GDPR as part of the wider data protection reform package which includes the proposed directive for police and judicial activities.

This opinion **updates the opinion published in March 2012** (which remains valid) to engage more directly with the positions of the co-legislators and to propose specific recommendations to assist the participants in the trilogue in reaching the right consensus on time.

A rare opportunity: the EDPS recalled that data protection reform is of central importance:

> **1. The EU is in the last mile of a marathon effort to reform its rules on personal information**. The General Data Protection Regulation will potentially affect, for decades to come, all individuals in the EU, all organisations in the EU who process personal data and organisations outside the EU who process personal data on individuals in the EU.
>
> **2. Effective data protection empowers the individual and galvanises responsible businesses and public authorities**. Laws in this area are complex and technical, requiring expert advice, in particular that of independent data protection authorities who understand the challenges of compliance. The GDPR is likely to be one of the longest in the Union's statute book, so now the EU must aim to be selective, focus on the provisions which are really necessary and avoid detail which as an unintended consequence might unduly interfere with future technologies. The texts of each of the institutions preach clarity and intelligibility in personal data processing: so the GDPR must practice what it preaches, by being as concise and easy to understand as possible.
>
> **3. The EU needs a new deal on data protection**. The rest of the world is watching closely. The quality of the new law and how it interacts with global legal systems and trends is paramount.
>
> **EDPS recommendations**: the options on the table, in the form of the respective texts preferred by the Commission, Parliament and Council, each contain many worthy provisions, but **each can be improved**.

The recommendations are driven by three abiding concerns:

- **a better deal for citizens**: for the EDPS, the starting point is the **dignity of the individual** which transcends questions of mere legal compliance. The point of reference is the principles at the core of data protection, that is, Article 8 of the Charter of Fundamental Rights. In this regard, the EDPS concentrated on the following issues:
- **clarify the term 'personal information'**: individuals should be able to exercise more effectively their rights with regard to any information which is able to identify or single them out, even if the information is considered 'pseudonymised';
- **all data processing must be both lawful and justified**: for instance: (i) personal data should only be used in ways compatible with the original purposes for collection; (ii) consent is one possible legal basis for processing, but it is necessary to prevent coercive tick boxes where there is

no meaningful choice for the individual and where there is no need for data to be processed at all; (iii) the EU should not open the door for direct access by third country authorities to data located in the EU;
- **more independent, more authoritative supervision**: (i) authorities should be able to hear and to investigated complaints and claims brought by data subjects or bodies, organisations and associations; (ii) individual rights enforcement requires an effective system of liability and compensation for damage caused by the unlawful data processing.

2. Rules which will work in practice: each of the three texts demands **greater clarity and simplicity** from those responsible for processing personal information. Equally, technical obligations must also be concise and easily-understood if they are to be implemented properly by controllers. This implies:

- **effective safeguards, not procedures**: the EDPS recommends a scalable approach which reduces documentation obligations on controllers into single policy on how it will comply with the regulation taking into account the risks, with compliance demonstrated transparently, whether for transfers, contracts with processors or breach notifications. It also recommends requiring notification of data breaches to the supervisory authority and data protection impact assessments only where the rights and freedoms of data subjects are at risk;
- **a better equilibrium between public interest and personal data protection**: data protection rules should not hamper historical, statistical and scientific research which is genuinely in the public interest;
- **trusting and empowering supervisory authorities**: supervisory authorities should be allowed to issue guidance to data controllers and to develop their own internal rules of procedure in the spirit of a simplified, easier application of the GDPR by one single supervisory authority (the '**One Stop Shop'**) close to the citizen ('**proximity'**).

3. Rules which will last a generation: it is reasonable to expect a similar timeframe before the next major revision of data protection rules, **perhaps not until the late 2030s**. Long before this time, data-driven technologies can be expected to have converged with artificial intelligence, natural language processing and biometric systems.

These technologies are challenging the principles of data protection. A future-oriented reform must therefore be predicated on the dignity of the individual and informed by ethics. It must redress the imbalance between innovation in the protection of personal data and its exploitation, making safeguards effective in our digitised society.

Faced with these challenges, the EDPS:

- considers that the **reform should reverse the recent trend towards secret tracking and decision making on the basis of profiles hidden from the individual;** fuller transparency from controllers is needed;
- strongly supports the introduction of the principles of data protection **by design and by default** as a means of kick-starting market-driven solutions in the digital economy;
- allows a **direct transfer of data** from one controller to another on the data subject's request and entitling data subjects to receive a copy of the data which they themselves can transfer to another controller.

Unfinished business: the EDPS noted that the adoption of a future-oriented EU data reform package will be an impressive but nonetheless incomplete achievement.

Directive 2002/58/EC (the 'ePrivacy Directive') will have to be amended.

The EU requires a **clear framework for the confidentiality of communications**, an integral element of the right to privacy, which governs all services enabling communications, not only providers of publicly available electronic communications. This must be done by means of a legally-certain and harmonising regulation.

At a time when people's trust in companies and governments has been shaken by revelations of mass surveillance and data breaches, the EDPS stresses that this confers considerable responsibility on EU law-makers whose decisions this year can be expected to have an impact not beyond Europe.

Personal data protection: processing and free movement of data (General Data Protection Regulation)

2012/0011(COD) - 14/04/2016

The European Parliament adopted a legislative resolution on the Council position at first reading with a view to the adoption of a regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Following the recommendation for second reading by the Committee on Civil Liberties, Justice and Home Affairs, Parliament **approved the Council position at first reading**, without amendment.

Personal data protection: processing and free movement of data (General Data Protection Regulation)

2012/0011(COD) - 10/10/2014

The Council reached a **partial general approach** on specific aspects of the draft regulation setting out a general EU framework for data protection. The partial general approach includes **chapter IV of the draft regulation (controller and processor),** on the understanding that:

- nothing is agreed until everything is agreed;
- it is without prejudice to any horizontal questions;
- it does not mandate the presidency to engage in informal trilogues with the European Parliament on the text.

Chapter IV was discussed intensively during the first half of 2013. Whilst at the Council meeting on 6-7 June 2013, all delegations congratulated the Irish Presidency on the very important progress achieved in this regard, a number of issues were still outstanding, in particular the need to further **reduce the administrative burden/compliance costs flowing from this Regulation by sharpening the risk-based approach**.

According to the approach, the likelihood and severity of the risk should be determined in function of the nature, scope, context and purposes of the data processing. **Risk should be evaluated on an objective assessment**, by which it is established whether data processing operations involve a high risk.

A high risk is a particular risk of prejudice to the rights and freedoms of individuals, in particular:

- where data processing which could lead to physical, material or moral damage, in particular where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of data protected by professional secrecy, [breach of (…) pseudonymity], or any other significant economic or social disadvantage;
- where data subjects might be deprived of their rights and freedoms or from exercising control over their personal data;
- where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions and offences or related security measures;
- where personal aspects are evaluated, in particular analysing and prediction of aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles;
- where personal data of vulnerable individuals, in particular of children, are processed;
- where processing involves a large amount of personal data and affects a large number of data subjects.

The orientation prescribed that **where a controller not established in the Union** is processing personal data of data subjects residing in the Union, the controller should designate a representative, **unless the processing it carries out is occasional** and unlikely to result in a risk for the rights and freedoms of data subjects, taking into account the nature, scope, context and purposes of the processing or the controller is a public authority or body.

The representative should be explicitly designated by a written mandate of the controller to act on its behalf with regard to the latter's obligations under this Regulation. The controller or processor should **maintain records** regarding all categories of processing activities under its responsibility.

In **assessing data security risk**, consideration should be given to the risks that are presented by data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed, which may in particular lead to physical, material or moral damage.

In order to enhance compliance with this Regulation in cases where the processing operations are likely to result in a high risk for the rights and freedoms of individuals, the controller [or the processor] should be responsible for the carrying out of a **data protection impact assessment to evaluate**, in particular, the origin, nature, particularity and severity of this risk.

Personal data protection: processing and free movement of data (General Data Protection Regulation)

2012/0011(COD) - 04/12/2014

The Council a **partial general approach** on specific issues of the draft regulation setting out a general EU framework for data protection, on the understanding that:

- **nothing is agreed until everything is agreed** and does not exclude future changes to be made to the text of the provisionally agreed Articles to ensure the overall coherence of the Regulation;
- it is without prejudice to any **horizontal questions**;
- it does not mandate the presidency to engage in informal **trilogues** with the European Parliament on the text.

The partial general approach includes some articles which are crucial to the question of the public sector (**Article 1** (subject matter and objectives), **Article 6** (lawfulness of processing), **Article 21** (restrictions)) as well as chapter IX (provisions relating to specific data processing situations).

The agreed text of Articles 1, 6, paragraphs (2) (3), and 21 and of the corresponding recitals now clearly **provides the framework within which Member States will be able to maintain and adopt legislation under this Regulation**. The Presidency believes that the text is a balanced one, granting Member States an appropriate measure of flexibility while maintaining a coherent structure of the Regulation.

The general approach comprises **Chapter XI on the provisions relating to specific data processing situations** (e.g. rules governing freedom of expression and information, access to official public documents, re-use of public information, for health purposes, such as public health and social protection and the management of health care services, derogations applicable to processing personal data for historical, statistical or scientific purposes and for archiving purposes).

The question whether and how to deal with processing of personal data by the public sector in the draft General Data Protection Regulation (GDPR) is one of particular sensitivity and importance to delegations. At the informal Ministerial Meeting in Milan on 9 July 2014 an overall majority of Member States supported a Regulation as legal instrument, but the need to provide Member States with sufficient leeway to determine the data protection requirements applicable to the public sector was equally emphasised.

The "one-stop-shop" mechanism: the Council also held a debate on the "one stop shop" mechanism on the basis of a proposal presented by the Presidency. A majority of ministers endorsed the general architecture of the proposal and concluded that further technical work will need to be done in the coming months on the basis of the guidelines set out at the 2013 October and December JHA Councils:

- in **important transnational cases** the draft Regulation should establish a one-stop shop mechanism in order to arrive at a single supervisory decision, which would be fast, ensure consistent application, provide legal certainty and reduce administrative burden;
- experts should explore methods for enhancing the "**proximity**" between individuals and the decision-making supervisory authority by involving the local supervisory authorities in the decision-making process;
- further work at technical level should include investigating the possibility of providing the **European Data Protection Board** in some cases with the power to adopt binding decisions regarding corrective measures.

Personal data protection: processing and free movement of data (General Data Protection Regulation)

2012/0011(COD) - 08/04/2016 - Council position

The Council adopted its position at first reading with a view to the adoption of a general data protection regulation. The proposed regulation aims to reinforce data protection rights of individuals, facilitate the free flow of personal data in the single market and reduce administrative burden, and harmonise the data protection rules in the European Union.

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.

The main points of the Council position at first reading are as follows:

Scope: the Council position 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.

Furthermore, the Council position **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). It 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**.

The main points in the Council position at first reading are as follows:

Principles relating to personal data processing: with a view to providing legal certainty, the Council position builds on the Directive 95/46 in specifying that processing of personal data is only lawful if at least one of the following conditions is fulfilled:

- the data subject has **clearly and explicitly consented** to the processing for one or more specific purposes; the Council Position provides for a specific protective regime for consent by children in relation to the offering of information society services;
- **the processing is necessary** for: (i) a contract; (ii) a legal obligation; (iii) protection of vital interests of the data subject or of another natural person; (iv) a task carried out in the public interest or in the exercise of official authority vested in the controller; (v) the legitimate interests pursued by a controller or by a third party.

The Council position:

- **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;
- 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.

Empowerment of data subjects: the Council position provides data subjects with reinforced data protection rights and by placing obligations on controllers. The rights of the data subject encompass:

- **the right to information:** controllers must provide information and communication in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed to a child;
- the right of **access** to personal data, i.e. 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;

- the right to **rectification**;
- the right to erasure of personal data, including a **"right to be forgotten"**;
- the right to **restriction** of processing;
- the right to data **portability**: 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
- the right to **object**, and the right not to be subject to a decision solely based on automated processing, including **profiling**. 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.

Controller and Processor: the Council position 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. The regulation lays down rules relating to the responsibilities of the controller concerning:

- impact assessments, where processing operations involve a high risk, for the rights and freedoms of individuals;
- keeping records of processing,
- data breaches,
- the designation of a Data Protection Officer, and
- codes of conducts and certification mechanisms.

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

Supervisory Authorities: 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.

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.

Remedies, liabilities and penalties: the regulation contains an elaborate set of rules that enables data subjects several avenues for remedies, including **claiming compensation** in case of damage as a result of infringement of the regulation.

In order to ensure compliance with the provisions of the regulation, the Council position provides that supervisory authorities can impose **administrative fines**, which go up to 20 million EUR or 4 % of the world-wide turnover of the infringer.