Basic information

2012/0010(COD) COD - Ordinary legislative procedure (ex-codecision procedure) Directive	Procedure completed
Personal data protection: processing of data for the purposes of prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties, and free movement of data Repealing Decision 2008/977/JHA, Framework Decision 2005/0202 (CNS) See also 2012/0011(COD) See also 2012/2874(RSP) **Subject** 1.20.09 Protection of privacy and data protection 7.30.05 Police cooperation 7.30.30 Action to combat crime 7.40.04 Judicial cooperation in criminal matters	

Key players

European Parliament

Committee responsible	Rapporteur	Appointed
LIBE Civil Liberties, Justice and Home Affairs	LAURISTIN Marju (S&D)	15/09/2014
	Shadow rapporteur VOSS Axel (PPE) IN 'T VELD Sophia (ALDE) ALBRECHT Jan Philipp (Verts/ALE) KIRKHOPE Timothy (ECR) ERNST Cornelia (GUE/NGL) WINBERG Kristina (EFD)	

Former committee responsible	Former rapporteur	Appointed
LIBE Civil Liberties, Justice and Home Affairs	DROUTSAS Dimitrios (S&D)	25/04/2012

Former committee for opinion	Former rapporteur for opinion	Appointed
JURI Legal Affairs	VOSS Axel (PPE)	14/06/2012

Council of the European Union	

Council configuration	Meetings	Date
Justice and Home Affairs (JHA)	3298	2014-03-03
Justice and Home Affairs (JHA)	3319	2014-06-05
Justice and Home Affairs (JHA)	3260	2013-10-07
Justice and Home Affairs (JHA)	3336	2014-10-09
Justice and Home Affairs (JHA)	3354	2014-12-05

European Commission

Commission DG	Commissioner
Justice and Consumers	REDING Viviane

Key events

Date	Event	Reference	Summary
25/01/2012	Legislative proposal published	COM(2012)0010	Summary
16/02/2012	Committee referral announced in Parliament, 1st reading		
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	A7-0403/2013	Summary
03/03/2014	Debate in Council		Summary
11/03/2014	Debate in Parliament		
12/03/2014	Decision by Parliament, 1st reading	T7-0219/2014	Summary
12/03/2014	Results of vote in Parliament		
05/06/2014	Debate in Council		
03/09/2014	Committee decision to open interinstitutional negotiations after 1st reading in Parliament		
09/10/2014	Debate in Council		
05/12/2014	Debate in Council		
17/12/2015	Approval in committee of the text agreed at 1st reading interinstitutional negotiations		
08/04/2016	Council position published	05418/1/2016	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	A8-0138/2016	Summary
13/04/2016	Debate in Parliament		
14/04/2016	Decision by Parliament, 2nd reading	T8-0126/2016	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	2012/0010(COD)
Procedure type	COD - Ordinary legislative procedure (ex-codecision procedure)
Procedure subtype	Legislation
Legislative instrument	Directive
Amendments and repeals	Repealing Decision 2008/977/JHA, Framework Decision 2005/0202(CNS) See also 2012/0011(COD) See also 2012/2874(RSP)
Legal basis	Treaty on the Functioning of the European Union TFEU 016-p2
Stage reached in procedure	Procedure completed
Committee dossier	LIBE/8/05251

Documentation gateway

European Parliament

Document type	Committee	Reference	Date	Summary
Committee draft report		PE501.928	20/12/2012	
Amendments tabled in committee		PE506.127	06/03/2013	
Amendments tabled in committee		PE506.128	08/03/2013	
Committee opinion	JURI	PE502.007	16/04/2013	
Committee report tabled for plenary, 1st reading/single reading		A7-0403/2013	22/11/2013	Summary
Text adopted by Parliament, 1st reading/single reading		T7-0219/2014	12/03/2014	Summary
Committee draft report		PE580.498	04/04/2016	
Committee recommendation tabled for plenary, 2nd reading		A8-0138/2016	12/04/2016	Summary
Text adopted by Parliament, 2nd reading		T8-0126/2016	14/04/2016	Summary

Council of the EU

Document type	Reference	Date	Summary
Council position	05418/1/2016	08/04/2016	Summary
Draft final act	00016/2016/LEX	27/04/2016	

European Commission

Document type	Reference	Date	Summary
Legislative proposal	COM(2012)0010	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	
Commission communication on Council's position	COM(2016)0213	11/04/2016	Summary
Follow-up document	COM(2020)0262	24/06/2020	
Follow-up document	COM(2022)0364	25/07/2022	

National parliaments

Document type	Parliament /Chamber	Reference	Date	Summary
Contribution	BE_CHAMBER	COM(2012)0010	12/04/2012	
Contribution	PT_PARLIAMENT	COM(2012)0010	12/04/2012	
Contribution	ES_PARLIAMENT	COM(2012)0010	12/05/2012	
Contribution	FR_ASSEMBLY	COM(2012)0010	12/05/2012	
Contribution	CZ_SENATE	COM(2012)0010	30/05/2012	
Contribution	IT_SENATE	COM(2012)0010	28/06/2012	
Contribution	RO_CHAMBER	COM(2012)0010	20/10/2012	
Contribution	EE_PARLIAMENT	COM(2012)0010	02/10/2013	

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

Additional information

Source	Document	Date
National parliaments	IPEX	
European Commission	EUR-Lex	
European Commission	EUR-Lex	

Final act
Directive 2016/0680 OJ L 119 04.05.2016, p. 0089 Summary Corrigendum to final act 32016L0680R(01) OJ L 127 23.05.2018, p. 0006-0007

Personal data protection: processing of data for the purposes of prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties, and free movement of data

2012/0010(COD) - 25/01/2012 - Legislative proposal

PURPOSE: to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data while guaranteeing a high level of public safety, and to ensure the exchange of personal data between competent authorities within the Union.

PROPOSED ACT: Directive 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 several instruments providing specific data protection rules in the area of police and judicial cooperation in criminal matters (ex-third pillar), including Framework Decision 2008/977/JHA.

Framework Decision 2008/977/JHA has a limited scope of application, since it only applies to cross-border data processing and not to processing activities by the police and judiciary authorities at purely national level. The Framework Decision leaves a large room for manoeuvre to Member States' national laws in implementing its provisions. Additionally, it does not contain any mechanism or advisory group similar to the Article 29 Working Party supporting common interpretation of its provisions, nor foresees any implementing powers for the Commission to ensure a common approach in its implementation.

Due to the **specific nature of the field of police and judicial co-operation in criminal matters**, it was acknowledged in Declaration 21 (annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon) that **specific rules on the protection of personal data and the free movement of such data in the fields of judicial co-operation in criminal matters and police co-operation based on Article 16 TFEU may prove necessary**.

- 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.
- In its resolution on the Stockholm Programme, the European Parliament welcomed a comprehensive data protection scheme in the EU and among others called for the revision of the Framework Decision. 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.

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
- **this 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: (i) improving the internal market dimension of data protection, (ii) making the exercise of data protection rights by individuals more effective and, (iii) creating a comprehensive and coherent framework covering all areas of Union competence, including police co-operation and judicial co-operation in criminal matters. As regards this latter objective in particular, two policy options were assessed:

- **a first one** basically extending the scope of data protection rules in this area and addressing the gaps and other issues raised by the Framework Decision,

- **and a second more far-reaching one** with very prescriptive and stringent rules, which would also entail the immediate amendment of all other "former third pillar" instruments.

A third "minimalistic" option based largely on interpretative Communications and policy support measures, such as funding programmes and technical tools, with minimum legislative intervention, was not considered appropriate to address the issues identified in this area in relation to data protection.

The analysis of the overall impact led to the development of the **preferred policy option** which is incorporated in the present proposal. According to the assessment, its implementation will lead to further strengthening data protection in this policy area in particular by including domestic data processing, thereby also enhancing legal certainty for competent authorities in the areas of judicial co-operation in criminal matters and police co-operation.

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

CONTENT: the proposed Directive repeals Framework Decision 2008/977/JHA. It defines the rules relating to processing of personal data for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal offences, and sets out the Directive's two-fold objective, i.e. to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data while guaranteeing a high level of public safety, and to ensure the exchange of personal data between competent authorities within the Union. It defines the scope of application of the Directive. The scope of the Directive is not limited to cross-border data processing but applies to all processing activities carried out by 'competent authorities' as defined in the Directive.

Principles: the proposal sets out the principles relating to processing of personal data and requires the distinction, as far as possible; between personal data of different categories of data subjects. It sets out the grounds for lawful processing, when necessary for the performance of a task carried out by a competent authority based on national law, to comply with a legal obligation to which the data controller is subject, in order to protect the vital interests of the data subject or another person or to prevent an immediate and serious threat to public security.

The proposed Directive sets out a **general prohibition of processing** special categories of personal data and the exceptions from this general rule. It establishes a prohibition of measures based solely on automated processing of personal data if not authorised by law providing appropriate safeguards.

Rights of the data subject: the proposal introduces the obligation for Member States to ensure easily accessible and understandable information, and to oblige controllers to provide **procedures and mechanisms for facilitating the exercise of the data subject's rights**. This includes the requirement that the exercise of the rights shall be in principle **free** of charge. It specifies the obligation for Member States to ensure the information towards the data subject. It also provides the obligation for Member States to ensure the data subject's **right of access** to their personal data.

The proposal provides that Member States may adopt **legislative measures restricting the right of access** if required by the specific nature of data processing in the areas of police and criminal justice, and on the information of the data subject on a restriction of access.

Provisions on the **rectification, erasure and restriction** of processing in judicial proceedings provide clarification based on Article 4(4) of Framework Decision 2008/977/JHA.

Controller and processor: the proposal sets out that the Member States must ensure the compliance of the controller with the obligations arising from the principles of data protection **by design and by default**. It clarifies the position and obligation of processors, and adds new elements, including that a processor that processes data beyond the controller's instructions is to be considered a co-controller. It introduces the obligation for controllers and processors to **maintain documentation** of all processing systems and procedures under their responsibility.

Data security: the Article on the security of processing is based on the current Article 17(1) of Directive 95/46 on the security of processing, and Article 22 of Framework Decision 2008/977/JHA, extending the related obligations to processors, irrespective of their contract with the controller.

The proposal introduces an **obligation to notify personal data breaches**, inspired by the personal data breach notification, clarifying and separating the obligations to notify the supervisory authority and to communicate, in qualified circumstances, to the data subject. It also provides for exemptions on reasons set out in the Directive.

Data Protection Officer: the proposal introduces an obligation for the controller to appoint a mandatory data protection officer who should fulfil the tasks listed in the Directive. Where several competent authorities are acting under the supervision of a central authority, functioning as controller, at least this central authority should designate such a data protection officer.

Transfer of personal data to third countries or international organisations: transfers to third countries may take place **only if the transfer is necessary** for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

The proposal lays down that transfers to a third country may take place in relation to which the Commission has adopted an adequacy decision of the level of protection or, in the absence of such decisions, where appropriate safeguards are in place. It furthermore sets out the criteria for the Commission’s assessment of an adequate or not adequate level of protection, and expressly includes the rule of law, judicial redress and independent supervision. It also provides for the possibility for the Commission to assess the level of protection afforded by a territory or a processing sector within a third country.

In addition, the proposed Directive:

- defines the **appropriate safeguards** needed prior to international transfers, in the absence of a Commission adequacy decision. These safeguards may be adduced by a legally binding instrument such as an international agreement. Alternatively, the data controller may on the basis of an assessment of the circumstances surrounding the transfer conclude that they exist;
- spells out the derogations for data transfer;
- obliges Member States to provide that the controller **informs the recipient of any processing restrictions** and takes all reasonable steps to ensure that these restrictions are met by recipients of the personal data in the third country or international organisation;
-

- explicitly provides for **international co-operation mechanisms** for the protection of personal data between the Commission and the supervisory authorities of third countries.

Independent national supervisory authorities: the proposal obliges Member States to establish supervisory authorities and to enlarge the mission of these authorities to contribute to the consistent application of the Directive throughout the Union, which may be the supervisory authority established under the General Data Protection Regulation. It clarifies the conditions for the independence of supervisory authorities, implementing case law of the Court of Justice.

It sets out the competence of the supervisory authorities. It obliges Member States to provide for the duties of the supervisory authority, including hearing and investigating complaints and promoting the awareness of the public on risk, rules, safeguards and rights. A particular duty of the supervisory authorities in the context of this Directive is, where direct access is refused or restricted, to **exercise the right of access on behalf of data subjects** and to check the lawfulness of the data processing.

Co-operation: the proposal introduces rules on mandatory mutual assistance. It provides that the European Data Protection Advisory Board, established by the General Data Protection Regulation, exercises its tasks also in relation to processing activities within the scope of this Directive.

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 of data for the purposes of prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties, and free movement of data

2012/0010(COD) - 07/03/2012

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:

- a proposal for a Regulation containing the general rules on data protection (COD/2012/0011) and
- this 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;
- ncorporate 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 of data for the purposes of prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties, and free movement of data

2012/0010(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 directive of the European Parliament and of the Council on the on the Council position at first reading with a view to the adoption of a directive of the European

Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

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 of data for the purposes of prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties, and free movement of data

2012/0010(COD) - 07/10/2013

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

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

- a 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
- this 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 of data for the purposes of prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties, and free movement of data

2012/0010(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 Dimitrios Droutsas (S&D, EL) on the 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.

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:

Minimum standards in the Directive: EU countries may set higher standards than those enshrined in the Directive.

Principles relating to personal data processing: personal data must be processed lawfully, fairly and in a transparent and verifiable manner in relation to the data subject. Such data must be adequate, relevant, and **limited to the minimum necessary** in relation to the purposes for which they are

processed. They shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data.

The controller must implement technical and organisational measures to prevent accidental loss, destruction or damage.

Access to data initially processed for other purposes: the committee added in a new Article stating that competent authorities may only have access to personal data initially processed for purposes other than those referred to in the text if they are specifically authorised by Union or Member State law which must meet the requirements set out.

Access is allowed only by **duly authorised staff** of the competent authorities in the performance of their tasks.

Time limits of storage and review: personal data processed **shall be deleted** by the competent authorities where they are no longer necessary for the purposes for which they were processed. Competent authorities must put mechanisms in place to **ensure that time-limits are established for the erasure of personal data** and for a periodic review of the need for the storage of the data, **including fixing storage periods for the different categories of personal data.** Procedural measures shall be established to ensure that those time limits or the periodic review intervals are observed.

Different categories of data subjects: the draft directive sets out provisions permitting processing of the personal data of the different categories of data subjects. Personal data of other data subjects than those referred to may only be processed under strict conditions only for as long as necessary for the investigation or for targeted, preventive purposes.

Different degrees of accuracy and reliability of personal data: personal data based on facts must be distinguished from personal data based on personal assessments, in accordance with their degree of accuracy and reliability. The committee states that personal data that are inaccurate, incomplete or no longer up to date must not transmitted or made available. To this end, the **competent authorities shall assess the quality of personal data** before they are transmitted or made available. As far as possible, in all transmissions of data, available information shall be added which enables the receiving Member State to assess the degree of accuracy, completeness, up-to-dateness and reliability. Personal data shall not be transmitted without request from a competent authority, in particular data originally held by private parties.

Members add that if it emerges that incorrect data have been transmitted or data have been transmitted unlawfully, the **recipient must be notified without delay** and is obliged to rectify the data or to erase them.

Lawfulness of processing: Member State law regulating the processing of personal data within the scope of this Directive shall contain explicit and detailed provisions specifying at least: (i) the objectives of the processing; (ii) the personal data to be processed; (iii) the specific purposes and means of processing; (iv) the appointment of the controller, or of the specific criteria for the appointment of the controller; (v) he categories of duly authorised staff of the competent authorities for the processing of personal data; (vi) the procedure to be followed for the processing; (vii) the use that may be made of the personal data obtained; (viii) limitations on the scope of any discretion conferred on the competent authorities in relation to the processing activities.

Profiling: the committee amendments strengthen safeguards against extensive profiling. Profiling remains permissible only under strict conditions. Automated processing of personal data intended to single out a data subject without an initial suspicion that the data subject might have committed or will be committing a criminal offence shall only be lawful to the extent that it is **strictly necessary for the investigation of a serious criminal offence** or the prevention of a clear and imminent danger, established on factual indications, to public security, the existence of the State, or the life of persons.

Data subjects are entitled to information about the logic used in the profiling and the **right to obtain human assessment**. Profiling that, whether intentionally or otherwise, has the effect of discriminating against individuals on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union membership, gender or sexual orientation, or that, whether intentionally or otherwise, results in measures which have such effect, shall be prohibited in all cases.

General principles for the rights of the data subject: such rights must include, inter alia, 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 his or her data**, the right to obtain data, 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.

Processing of genetic data for the purpose of a criminal investigation or a judicial procedure: the committee added provisions stating that genetic data may only be used to establish a genetic link within the framework of adducing evidence, preventing a threat to public security or preventing the commission of a specific criminal offence. They may **not be used to determine other characteristics** which may be linked genetically.

Such data may only be retained as long as necessary for the purposes for which data are processed and where the individual concerned has been convicted of serious offences against the life, integrity or security of persons, subject to **strict storage periods to be determined by Member State law.**

Data transferred to third countries: data transferred to competent public authorities in third countries should not be further processed for purposes other than the one they were transferred for. Further onward transfers from competent authorities in third countries or international organisations to which personal data have been transferred should **only be allowed if the onward transfer is necessary for the same specific purpose as the original transfer** and the **second recipient is also a competent public authority**. Further onward transfers should not be allowed for general law-enforcement purposes.

Derogations to these rules are set out in the report.

Powers: the report expands on the powers of supervisory authorities, which now include: (i) warning or admonishing the controller or the processor; (ii) ordering the rectification, erasure or destruction of all data when they have been processed in breach of the provisions; (iii) imposing a temporary or definitive ban on processing; (iv) informing national parliaments, the government or other public institutions as well as the public on the matter.

The report also **expands the supervisory authority's investigative power** to obtain from the controller or the processor certain information laid out in the text.

Each supervisory authority shall have the power to **impose penalties in respect of administrative offences.**

Data protection officer: he or she shall be appointed for a period of at least **four years** and may be reappointed for further terms. The data protection officer may only be dismissed from that function, if he or she no longer fulfils the conditions required for the performance of his or her duties.

Reporting of violations: Members stipulate that supervisory authorities must take into account guidance issued by the European Data Protection Board and, together with competent authorities, put in place effective mechanisms to encourage **confidential reporting of breaches** of the Directive.

Joint operations: where these take place, in cases where data subjects in other Member States are likely to be affected by processing operations, the competent supervisory authority may be invited to participate in the joint operations. It may invite the supervisory authority of each of those Member States to take part in the respective operation and in cases where it is invited, respond to the request of a supervisory authority to participate in the operations without delay.

Transmission of personal data to other parties: a new Chapter VIIIa states that the controller must not transmit or instruct the processor to transmit personal data to a natural or legal person not subject to the provisions adopted pursuant to the Directive, unless the prescribed conditions are met. These include the condition that the recipient is established in a Member State of the EU, and no legitimate specific interests of the data subject prevent transmission.

Personal data protection: processing of data for the purposes of prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties, and free movement of data

2012/0010(COD) - 03/03/2014

The Council was briefed by the Presidency on the **state of play** regarding the 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.

This debate follows a long series of work carried out by several successive Presidencies up until the current Greek Presidency.

Need for and scope of the instrument: several delegations have reservations on the need to replace the Framework Decision with a new instrument covering not only cross-border data processing operations but also domestic processing operations. Some delegations also point to difficulties linked to the possible delineation between the proposed Regulation and Directive. This is connected in particular with requests that the scope of the Directive covers the processing of personal data for the purpose of **ensuring public order** which are currently covered by Directive 95/46/EC even if the activities of public order are not undertaken for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

The current compromise provides that it applies to the processing of personal data by competent public authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences and for these purposes, the maintenance of public order, or the execution of criminal penalties.

Further alignment with the General Data Protection Regulation: there is a large support for carrying over in the Directive some of the solutions found within the context of the General Data Protection Regulation as regards definitions of the Directive (Article 3), rights of the data subjects (Chapter III), obligations of controller and processor (Chapter IV for example Articles 28 and 29 on communication of data breach to supervisory authority and data subject), international transfers (Chapter V removal of negative adequacy) or independent supervisory authorities (Chapter VI).

Imposition of specific conditions: the proposed compromise provides that a Member State may impose specific processing conditions for the transfer of data has also been introduced following the approach of Article 12 of the Framework Decision. On this basis, where Union or Member State law applicable to the transmitting competent public authority provides for specific conditions to the processing of personal data, the transmitting public authority will inform the recipient about these conditions and the requirement to respect them.

Processing sensitive data: the Articles on lawfulness of processing and on processing for sensitive data (Articles 7 and 8) have been further clarified in the Presidency compromise. Some delegations further request the introduction of consent as ground for processing and to replace the rule of prohibition to process sensitive data (with listed exemptions) by an authorisation to process under specific conditions.

The provisions on the right of direct and indirect access of the individual to his/her personal data together with those on rights of the data subject in criminal investigations and proceedings reflect to a large extent the current Framework Decision. The discussion has shown that these provisions are still being questioned by several delegations.

Delegations have raised questions on other issues like the definition of "international organisations".

International transfers of data: Chapter V on International transfers has also been revised, for example as regards the introduction of a requirement that in case where personal data are transmitted or made available from another Member State, that Member State must give its prior authorisation to the transfer pursuant to its national law. The current compromise maintains the obligation imposing on Member States to eliminate the incompatibilities resulting from bilateral agreements not compatible with Union law (including by renegotiating incompatible agreements) but no longer foresees a fixed period of time upon Member States to amend the agreements.

The Greek Presidency will continue work on the text of the draft Directive.

Personal data protection: processing of data for the purposes of prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties, and free movement of data

2012/0010(COD) - 12/03/2014 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 371 votes to 276 with 30 abstentions, a legislative resolution on the 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.

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

Minimum standards in the Directive: the Directive should protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of their personal data and privacy. It should not preclude Member States from providing higher safeguards than those it established.

Principles: personal data must be: (i) processed lawfully, fairly and in a transparent and verifiable manner in relation to the data subject; (ii) only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data; (iii) processed in a way that effectively allows the data subject to exercise his or her rights; (iv) processed in a way that protects against unauthorised or unlawful processing and against accidental loss, destruction or damage; (v) processed by only those duly authorised staff of the competent authorities who need them for the performance of their tasks.

Personal data held by private parties or other public authorities shall only be accessed to investigate or prosecute criminal offences in accordance with necessity and proportionality requirements to be defined by Union law by each Member State in its national law.

Time limits of storage and review: personal data processed shall be deleted by the competent authorities where they are no longer necessary for the purposes for which they were processed. Competent authorities must put mechanisms in place to ensure that time limits are established for the erasure of personal data and for a periodic review of the need for the storage of the data.

Different categories of data subjects: competent authorities may process personal data of different categories of data subjects. Personal data of other data subjects may only be processed under certain conditions, for example, when such processing is indispensable for targeted, preventive purposes or the investigation or prosecution of a specific criminal offence.

Degrees of accuracy and reliability of personal data: personal data based on facts must be distinguished from personal data based on personal assessments, in accordance with their degree of accuracy and reliability. Personal data that are inaccurate, incomplete or no longer up to date must not transmitted or made available. They shall not be transmitted without request from a competent authority, in particular data originally held by private parties.

If it emerges that incorrect data have been transmitted or data have been transmitted unlawfully, the recipient must be notified without delay and is obliged to rectify the data or to erase them.

Lawfulness of processing: the processing of personal data is lawful only if and to the extent that processing is based on Union or Member State law. Parliament stated that national law regulating the processing of personal data within the scope of this Directive shall contain explicit and detailed provisions specifying at least: (i) the objectives of the processing; (ii) the personal data to be processed; (iii) the specific purposes and means of processing; (iv) the appointment of the controller; (v) the categories of duly authorised staff of the competent authorities for the processing of personal data; (vi) the procedure to be followed for the processing; (vii) the use that may be made of the personal data obtained; (viii) limitations on the scope of any discretion conferred on the competent authorities in relation to the processing activities.

Profiling: Members added a definition of profiling and strengthen safeguards for persons concerned. Automated processing of personal data intended to single out a data subject without an initial suspicion that the data subject might have committed a criminal offence shall only be lawful to the extent that it is strictly necessary for the investigation of a serious criminal offence or the prevention of a clear and imminent danger, established on factual indications, to public security, the existence of the State, or the life of persons.

Data subjects are entitled to information about the logic used in the profiling and the right to obtain human assessment. Such processing should in no circumstances contain, generate, or discriminate based on special categories of data regarding race or ethnic origin, political opinions, religion or beliefs, trade union membership, gender or sexual orientation.

General principles for the rights of the data subject: the directive should aim to strengthen, ensure, clarify and if necessary, codify these rights. Such rights must include, inter alia: (i) 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 his or her data, (ii) the right to obtain data, (iii) the right to lodge a complaint with the competent data protection authority and to bring legal proceedings as well as (iv) the right to compensation and damages resulting from an unlawful processing operation. Such rights shall in general be exercised free of charge.

Processing of genetic data: Parliament introduced new provisions stating that genetic data may only be used to establish a genetic link within the framework of adducing evidence, preventing a threat to public security or preventing the commission of a specific criminal offence. Such data may only be retained as long as necessary for the purposes for which data are processed and where the individual concerned has been convicted of serious offences against the life, integrity or security of persons, subject to strict storage periods to be determined by Member State law.

Data transferred to third countries: Parliament considered that the Commission proposal did not contain the safeguards necessary to protect the rights of persons whose data had been transferred. The amended text provided that where the Commission decides that a third country, or a territory within that third country, or an international organisation does not ensure an adequate level of protection, a controller or processor may not transfer personal data to a third country, or an international organisation **unless the controller or processor has adduced appropriate safeguards** with respect to the protection of personal data in a legally binding instrument.

These transfers must be **authorised by the supervisory authority prior to the transfer.**

Powers: Parliament strengthened the powers of supervisory authorities. The latter must have the same duties and effective powers in each Member State, including effective powers of investigation, power to access all personal data and all information necessary for the performance of each supervisory function, power to access any of the premises of the data controller or the processor including data processing requirements.

Supervisory authorities include: (i) warning or admonishing the controller or the processor; (ii) ordering the rectification, erasure or destruction of all data when they have been processed in breach of the provisions; (iii) imposing a temporary or definitive ban on processing; (iv) informing national parliaments, the government or other public institutions as well as the public on the matter.

Each supervisory authority shall have the power to impose penalties in respect of administrative offences.

Transmission of personal data to other parties: Parliament introduced a new Chapter which provided that the controller must not transmit personal data to a natural or legal person not subject to the provisions adopted pursuant to the Directive, such as: (i) the transmission complies with Union or national law; (ii) he recipient is established in a Member State of the European Union; (iii) no legitimate specific interests of the data subject prevent transmission.

Personal data protection: processing of data for the purposes of prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties, and free movement of data

2012/0010(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 Marju LAURISTIN (S&D, EE) on the Council position at first reading with a view to the adoption of a directive of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

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

To recall, the proposed directive will repeal Council Framework Decision 2008/977/JHA. Its objective is to ensure effective judicial cooperation in criminal matters and police cooperation and facilitate the exchange of personal data between competent authorities of the Member States while guaranteeing a consistent high level of protection of the personal data of natural persons.

Personal data protection: processing of data for the purposes of prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties, and free movement of data

2012/0010(COD) - 08/04/2016 - Council position

The Council adopted its position at first reading with a view to the adoption of a Directive of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data. It is part of a series of measures on data protection, which also includes a General Data Protection Regulation, and aims to replace Council Framework Decision 2008/977 /JHA.

The objective of the draft directive is **to ensure effective judicial cooperation in criminal matters and police cooperation** and facilitate the exchange of personal data between competent authorities of the Member States while guaranteeing a consistent high level of protection of the personal data of natural persons.

The Council position at first reading maintains the objectives of the Framework Decision, notably the **minimum harmonisation principle** from the Framework Decision. It contains clearer and more specific provisions on most of the provisions in the Framework Decision, in particular the provisions on transfers to third countries or international organisations. Furthermore, it aligns the text of the draft directive to that of draft regulation on a number of provisions. This is particularly the case with regard to definitions, the principles, the Chapter on the controller and processor, the adequacy decisions as well the Chapter on independent supervisory authorities.

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

Scope: the material scope of the draft directive encompasses the processing of personal data by competent authorities **for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security**. The draft directive, unlike the Framework Decision 2008/977/JHA, also applies to **domestic processing** of personal data.

As regards the scope of bodies to which the text applies, the Council position has expanded this beyond competent public authorities **to such bodies or entities** that have been entrusted by Member State law to exercise authority and public powers for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

Principles relating to personal data: the Council Position includes the notion of **transparency** among the recitals, while making clear that activities such as covert investigations or video surveillance will be allowed to take place. It adds that personal data should be processed in a manner that ensures appropriate **security** of the data, which includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Further processing: the Council position lays down that processing by the same or another controller for any of the purposes set out in the directive other than the one for which the personal data were collected, is only permitted where the controller is **authorised** to process such personal data for such purpose in accordance with Union or Member State law and the processing is **necessary and proportionate** to that other purpose.

Time limits of storage and review: the Council position lays down that appropriate time limits must be established for the erasure of personal data or for a periodic review of personal data that are stored to verify if it is necessary that they are kept.

Different categories of data subjects: Member States must, where applicable and as far as possible, provide for the controller to make a clear distinction between personal data of different categories of data subjects.

Lawfulness of processing: processing of personal data is lawful only if and to the extent that processing is **necessary** for the performance of a task carried out by a competent authority for the purposes set out in the directive and is based on Union or Member State law.

The main rule is that personal date collected at the beginning by a competent authority for the purposes set out in the directive may only be processed for one of the purposes in the directive.

Special categories of personal data: the Council position at first reading allows processing of such data but only where strictly necessary and on the condition that appropriate safeguards for the rights and freedoms of the data subject are adduced. In addition, such processing is allowed only where authorised in EU or Member State law to protect the vital interest of the data subject or where the processing relates to data that have manifestly been made public by the data subject.

Automated individual decision-making, including profiling: a decision based solely on automatic processing, including profiling, which produces an adverse legal effect for the data subject or that significantly affects him or her, must be prohibited unless Union or Member States law authorises it and appropriate safeguards for the rights and freedoms of the data subject are adduced.

Data subjects' rights: the new rules include:

- the right to be informed in a concise and intelligible manner, that his data are being processed;
- the right to have the identity and contact details of the controller and the purpose of the processing;
- the right of access to personal data and the duly justified restrictions to that right;
- the right to rectify, erase or restrict the processing of his or her personal data.

Controller and processor: the draft directive will be applied by competent authorities either domestically or when transmitting personal data between EU Member States or transferring personal data to third countries or international organisations. The provisions of the draft directive will be applied by public authorities and, under certain circumstances, private bodies.

Impact assessment: an impact assessment is necessary before the controller can carry out a processing where the processing is likely to result in a high risk for the rights and freedoms of natural persons. The draft directive sets out the situations in which an impact assessment is compulsory.

Transfers: in order to exchange data with third countries and international organisations, the Council position sets out rules on transfers. When data are transmitted or made available from another Member State, that Member State must give its prior authorisation. The Council position also lays down that all provisions on transfers must be applied in order to ensure that the level of protection of natural persons guaranteed in the draft directive are not undermined.

Furthermore, it adds the possibility for competent authority, but only those that are public authorities (and not the bodies or entities entrusted by Member State law to exercise public powers), to transfer personal data to recipients established in third countries.

Supervisory authorities: in order to ensure compliance with the rules of the draft directive, the monitoring of the latter as well as the draft regulation will be carried out by supervisory authorities.

Personal data protection: processing of data for the purposes of prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties, and free movement of data

2012/0010(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.

To recall, the draft directive for police and criminal justice authorities forms part of a Data Protection Reform package proposed by the Commission, which also comprises a General Data Protection Regulation.

It aims to repeal Framework Decision 2008/977/JAI in order to ensure a consistent high level of protection of the personal data of natural persons and facilitate the exchange of personal data between competent authorities of the Member States, in order to ensure effective judicial cooperation in criminal matters and police cooperation. The directive will enable law enforcement and judicial authorities to cooperate more effectively and rapidly with each other, and build confidence and ensure legal certainty.

The Commission notes that the agreement:

- maintains the overall objective to ensure **a high level of protection of personal data** in the field of police and judicial cooperation in criminal matters and to facilitate exchanges of personal data between Member States' police and judicial authorities, by applying harmonised rules also to data processing operations at the domestic level;
- **preserves the application of the general data protection principles** to police cooperation and judicial cooperation in criminal matters, while respecting the specific nature of these fields;
- clarifies the **material scope** of the directive by specifying that the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties include the "safeguarding against and the prevention of threats to public security";
- includes certain **private entities** in the notion of 'competent authorities' but such possibility is strictly limited to entities entrusted by national law to perform public authority or public powers for the purposes of the directive;
- provides for **minimum harmonised criteria** and conditions on possible limitations to the general rules. This concerns, in particular, the rights of individuals to be informed when police and judicial authorities handle or access their data;
- establishes a **distinction between different categories** of data subjects whose rights may vary (such as witnesses and suspects);
- strengthens the **risk based approach** by providing for the new obligation of the controller to carry out, in certain circumstances, a data protection impact assessment while maintaining the obligations related to data protection by design and by default and to the designation of a data protection officer;
- sets outs the rules for **international transfers to third countries** by authorities competent for the purposes of the Directive to such authorities, while providing also for the possibility of transfers to private bodies, subject to a number of specific conditions.

Accordingly, the Commission can accept the position adopted by Council in first reading.

Personal data protection: processing of data for the purposes of prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties, and free movement of data

2012/0010(COD) - 27/04/2016 - Final act

PURPOSE: to ensure effective judicial cooperation in criminal matters and police cooperation and to facilitate the exchange of personal data between competent authorities of Member States, whilst ensuring a consistent and high level of protection of the personal data of natural persons (reform of data protection).

LEGISLATIVE ACT: Directive (EU) 2016/680 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

CONTENT: the new Directive aims to **protect personal data that is processed for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties,** including the safeguarding against and the prevention of threats to public security. It responds to the need to ensure a high and systematic level of data protection for natural persons whilst at the same time facilitating the exchange of these data between the law enforcement services of different Member States.

The reform of data protection also includes a new General Data Protection Regulation (intended to replace 95/46/EC).

The main elements of the Directive are as follows:

Scope: the Directive 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 **cross-border processing** of personal data as well as processing of this data at national level.

The directive applies **not only to competent public authorities but also to any other body or entity** entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

Principles relating to processing of personal data: Member States shall provide for personal data to be:

- processed lawfully and fairly;
- collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;
- adequate, relevant and not excessive in relation to the purposes for which they are processed;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed; 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, using appropriate technical or organisational measures.

Processing purposes: the Directive provides that processing by the same or another controller for any of the purposes set out in the directive other than that for which the personal data are collected shall be **permitted in so far as the controller is authorised to process such personal data for such a purpose** in accordance with Union or Member State law, and that processing is necessary and proportionate to that other purpose.

Time-limits for storage and review: Member States shall provide for appropriate time limits to be established for the erasure of personal data or for a periodic review of the need for the storage of personal data. Procedural measures shall ensure that those time limits are observed.

Categories of data subject: Member States shall provide for the controller, where applicable and as far as possible, to make a clear distinction between personal data of different categories of data subjects.

Lawfulness of processing: processing shall be lawful only if it is **necessary** to carry out a particular task by a competent authority, for the purposes set out in the Directive, in accordance with Union or Member State law.

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 **allowed only where strictly necessary**, subject to appropriate safeguards for the rights and freedoms of the data subject.

A decision based solely on **automated processing, including profiling**, which produces an adverse legal effect concerning the data subject or significantly affects him or her, is prohibited unless authorised by Union or Member State law and unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Rights of the data subject: the new rules include:

- the right of the subject to be **informed**, in clear and simple terms, that the data concerning him are being processed;
- the right of the data subject to be informed about the identity and the contact details of the controller and the purposes of the processing for which the personal data are intended;
- the right of **access** by the data subject to personal data and the grounds for being refused access to that information;
- the right to **rectification or erasure** of personal data concerning the data subject or restriction on processing of such data.

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.

The new Directive provides that the controller shall designate **a data protection officer** to assist the supervisory authority on issues relating to processing.

Impact assessment: the impact assessment constitutes a tool to ensure that the provisions are observed. The controller should carry out a data protection impact assessment where the processing operations, in particular using new technologies, are likely to result in a high risk to the rights and freedoms of data subjects.

The controller or processor should consult the supervisory authority prior to processing which will form part of a new filing system to be created where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

Transfers of personal data outside the EU: the new rules also cover the transfer of personal data to a third country or to an international organisation. This transfer may only take place where the **Commission decides** that the third country or an international organisation ensures an adequate level of protection. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the rule of law, respect for human rights and fundamental freedoms, and the existence and effective functioning of one or more independent supervisory authorities in the third country.

Where personal data are transmitted from another Member State, that Member State must have given its prior authorisation to the transfer. Transfers from another Member State without prior authorisation will be permitted only when the transfer is necessary to prevent an immediate and serious threat to public security of a Member State or a third country or to essential interests of a Member State and the prior authorisation cannot be obtained in good time.

Supervisory authority: in order to ensure compliance with the rules of the Directive, supervisory authorities will carry out monitoring of the application of the Directive.

Liability and sanctions: the new Directive also gives data subjects the right to effective judicial redress against a prejudicial decision by a supervisory authority and the right to obtain compensation in case of damage following a breach of the Regulation.

ENTRY INTO FORCE: 5.5.2016.

TRANSPOSITION: by 6.5.2018. A Member State may provide, exceptionally, where it involves disproportionate effort, for automated processing systems set up before 6 May 2016 to be brought into conformity with Article 25(1) by 6 May 2023.