### Basic information

**COD - Ordinary legislative procedure (ex-codecision procedure)**

**Regulation**

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

Repealing Directive 95/46/EC 1990/0287(COD)


See also 2012/0010(COD)

**Subject**

1.10 Fundamental rights in the Union, Charter
1.20.09 Protection of privacy and data protection
2.80 Cooperation between administrations
3.45.05 Business policy, electronic commerce, after-sales service, commercial distribution
4.60.06 Consumers' economic and legal interests

**Selected topics**

Data protection

### Key players

**European Parliament**

<table>
<thead>
<tr>
<th>Committee responsible</th>
<th>Rapporteur</th>
<th>Appointed Date</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LIBE</strong> Civil Liberties, Justice and Home Affairs</td>
<td>Verts/ALE ALBRECHT Jan Philipp</td>
<td>12/04/2012</td>
</tr>
<tr>
<td></td>
<td>Shadow rapporteur</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PPE VOSS Axel</td>
<td></td>
</tr>
<tr>
<td></td>
<td>S&amp;D DROUTSAS Dimitrios</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ALDE ALVARO Alexander</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ECR KIRKHOPE Timothy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>GUE/NGL ERNST Cornelia</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Committee for opinion</th>
<th>Rapporteur for opinion</th>
<th>Appointed Date</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ECON</strong> Economic and Monetary Affairs</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>EMPL</strong> Employment and Social Affairs</td>
<td>ALDE HIRSCH Nadja</td>
<td>20/04/2012</td>
</tr>
<tr>
<td><strong>ITRE</strong> Industry, Research and Energy</td>
<td>PPE KELLY Seán</td>
<td>14/03/2012</td>
</tr>
<tr>
<td><strong>IMCO</strong> Internal Market and Consumer Protection</td>
<td>PPE COMI Lara</td>
<td>29/02/2012</td>
</tr>
<tr>
<td><strong>JURI</strong> Legal Affairs</td>
<td>PPE GALLO Marielle</td>
<td>14/06/2012</td>
</tr>
</tbody>
</table>

**Council of the European Union**

<table>
<thead>
<tr>
<th>Council configuration</th>
<th>Meeting</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justice and Home Affairs (JHA)</td>
<td>3354</td>
<td>04/12/2014</td>
</tr>
<tr>
<td>Justice and Home Affairs (JHA)</td>
<td>3336</td>
<td>10/10/2014</td>
</tr>
<tr>
<td>Justice and Home Affairs (JHA)</td>
<td>3298</td>
<td>03/03/2014</td>
</tr>
<tr>
<td>Justice and Home Affairs (JHA)</td>
<td>3279</td>
<td>06/12/2013</td>
</tr>
<tr>
<td>Justice and Home Affairs (JHA)</td>
<td>3260</td>
<td>07/10/2013</td>
</tr>
<tr>
<td>Justice and Home Affairs (JHA)</td>
<td>3244</td>
<td>06/06/2013</td>
</tr>
<tr>
<td>Justice and Home Affairs (JHA)</td>
<td>3195</td>
<td>25/10/2012</td>
</tr>
</tbody>
</table>

**European Commission**

<table>
<thead>
<tr>
<th>Commission DG</th>
<th>Commissioner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justice</td>
<td>REDING Viviane</td>
</tr>
</tbody>
</table>
## Key events

<table>
<thead>
<tr>
<th>Date</th>
<th>Event Description</th>
<th>Document Reference</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>25/01/2012</td>
<td>Legislative proposal published</td>
<td>COM(2012)0011</td>
<td>Summary</td>
</tr>
<tr>
<td>16/02/2012</td>
<td>Committee referral announced in Parliament, 1st reading/single reading</td>
<td></td>
<td></td>
</tr>
<tr>
<td>25/10/2012</td>
<td>Debate in Council</td>
<td>3195</td>
<td>Summary</td>
</tr>
<tr>
<td>06/06/2013</td>
<td>Debate in Council</td>
<td>3244</td>
<td></td>
</tr>
<tr>
<td>07/10/2013</td>
<td>Debate in Council</td>
<td>3260</td>
<td></td>
</tr>
<tr>
<td>21/10/2013</td>
<td>Vote in committee, 1st reading/single reading</td>
<td></td>
<td></td>
</tr>
<tr>
<td>22/11/2013</td>
<td>Committee report tabled for plenary, 1st reading/single reading</td>
<td>A7-0402/2013</td>
<td>Summary</td>
</tr>
<tr>
<td>06/12/2013</td>
<td>Debate in Council</td>
<td>3279</td>
<td></td>
</tr>
<tr>
<td>03/03/2014</td>
<td>Debate in Council</td>
<td>3298</td>
<td></td>
</tr>
<tr>
<td>12/03/2014</td>
<td>Results of vote in Parliament</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12/03/2014</td>
<td>Decision by Parliament, 1st reading/single reading</td>
<td>T7-0212/2014</td>
<td>Summary</td>
</tr>
<tr>
<td>10/10/2014</td>
<td>Debate in Council</td>
<td>3336</td>
<td>Summary</td>
</tr>
<tr>
<td>04/12/2014</td>
<td>Debate in Council</td>
<td>3354</td>
<td>Summary</td>
</tr>
</tbody>
</table>

## Technical information

- **Procedure reference**: 2012/0011(COD)
- **Procedure type**: COD - Ordinary legislative procedure (ex-codecision procedure)
- **Procedure subtype**: Legislation
- **Legislative instrument**: Regulation
  - Repealing Directive 95/46/EC 1990/0287(COD)
  - See also 2012/0010(COD)
- **Legal basis**: Treaty on the Functioning of the EU TFEU 114-p1; Treaty on the Functioning of the EU TFEU 016-p2
- **Modified legal basis**: Rules of Procedure of the European Parliament EP 150
- **Mandatory consultation of other institutions**: Economic and Social Committee
- **Stage reached in procedure**: Awaiting Council 1st reading position / budgetary conciliation convocation
- **Committee dossier**: LIBE/7/08739

## Documentation gateway

<table>
<thead>
<tr>
<th>Legislative proposal</th>
<th>Document Reference</th>
<th>Date</th>
<th>EC</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>COM(2012)0011</td>
<td>25/01/2012</td>
<td>EC</td>
<td>Summary</td>
</tr>
</tbody>
</table>
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.


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.
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 Commissions 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 Commissions 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.

2012/0011(COD) - 25/10/2012 Debate in Council

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.

2012/0011(COD) - 07/10/2013 Debate in Council

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
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).

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 Parliaments 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 subjects 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 Commissions 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 subjects 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.

2012/0011(COD) - 06/12/2013 Debate in Council

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
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.

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 subjects 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 subjects 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 controllers 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 persons 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.

2012/0011(COD) - 10/10/2014 Debate in Council

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.

2012/0011(COD) - 04/12/2014 Debate in Council

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.