

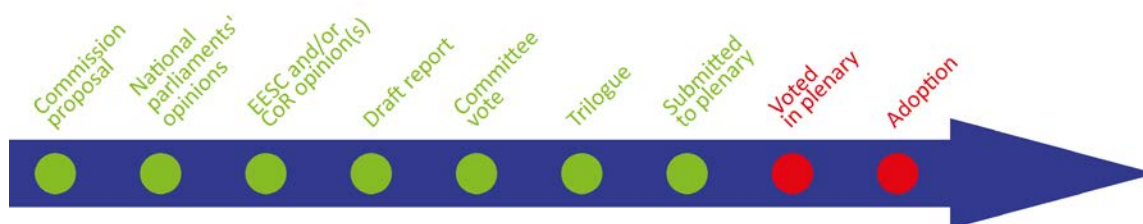
Rules for EU institutions' processing of personal data

OVERVIEW

In the context of the comprehensive reform of the EU's legal framework for data protection, the Commission tabled a proposal in January 2017 for a 'regulation on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and the free movement of such data' and repealing the existing one (Regulation No 45/2001). The aim is to align it to the 2016 General Data Protection Regulation (GDPR) that has been fully applicable since 25 May 2018. Interinstitutional trilogue meetings, in which debate focused on also applying the regulation to operational data of EU bodies carrying out law enforcement activities, brought an agreement between the co-legislators in May. The compromise text is due to be voted by the Parliament in the September plenary session.

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 by the Union institutions, bodies, offices and agencies and the free movement of such data and repealing Regulation(EC) No 45/2001 and Decision No 1247/2002/EC

<i>Committee responsible:</i>	Civil Liberties, Justice and Home Affairs (LIBE)	COM(2017) 8 10.1.2017
<i>Rapporteur:</i>	Cornelia Ernst (GUE/NGL, Germany)	2017/0002(COD)
<i>Shadow rapporteurs :</i>	Axel Voss (EPP, Germany) Marju Lauristin (S&D, Estonia) John Procter (ECR, United Kingdom) Angelika Mlinar (ALDE, Austria) Jan Philipp Albrecht (Greens/EFA, Germany)	Ordinary legislative procedure (COD) (Parliament and Council on equal footing – formerly 'co-decision')
<i>Next steps expected:</i>	First-reading vote in plenary	



Introduction

Among other initiatives in the field of data protection, and together with the proposed [e-Privacy regulation](#), in January 2017 the Commission adopted a [proposal](#) for a regulation on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and the free movement of such data. The aim is to reform the existing 2001 rules ([Regulation No 45/2001](#)) to align them to the 2016 [General Data Protection Regulation \(GDPR\)](#),¹ that is, to ensure that EU institutions and bodies processing personal data uphold individuals' rights, in accordance with the GDPR as well as with the e-Privacy rules (currently also [under review](#)). The aim of the present proposal (originally planned to be in force at the same time as the GDPR) is to provide citizens, companies and institutions with a consistent legal regime on data protection.

Context

Privacy and data protection are fundamental rights enshrined in EU primary and secondary law. Article 8 of the [Charter of Fundamental Rights](#) (CFR) states that everyone has the right to personal data protection; such personal data must be processed fairly, for specified purposes, and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Moreover, compliance with these rules is subject to control by an independent authority. The protection of natural persons in relation to the processing of their personal data is also enshrined in Article 16 of the Treaty on the Functioning of the EU ([TFEU](#)), as introduced by the Lisbon Treaty, which constitutes a specific legal basis for adopting legislative acts on data protection.²

The main current general data protection instrument in EU secondary law is the [GDPR](#), which has replaced the [Data Protection Directive \(95/46/EC\)](#)¹ since 25 May 2018 and contains general principles and rules to apply when private or public entities process personal data (e.g. conditions for lawful data processing, obligations and rights deriving from data processing and safeguards). The right to data protection also applies to the processing of personal data by EU institutions and bodies; however, ad hoc rules exist with [Regulation No 45/2001](#) on data processed by the EU institutions. The GDPR, excluding the latter from its scope, calls for Regulation 45/2001 to be adapted to its stronger rules.³ Updating the current legislation also appears necessary due to the advances in digital technologies.

Existing situation

At present, the rules on the protection of personal data processed by EU institutions and bodies are provided by Regulation 45/2001, which, as mentioned above, applies the main principles of the 1995 general data protection directive and which the new proposal aims to review. Its objectives are, on the one hand, to ensure effective protection of individuals' rights and, on the other, to allow the free flow of data between Member States and the institutions and among the institutions themselves, supported by an effective independent supervisory system.

Actors

In addition to the **data-subject** (i.e. the person whose data are collected, stored or otherwise processed by an EU institution as well as its staff), other main actors currently involved are: the **data controller**, which, under Regulation 45/2001, is the institution or body, the directorate-general, the unit or any other entity which, alone or jointly with others, determines how and for what purposes data are processed; the **data processor**, i.e. the natural or legal person or public body processing data on behalf of the controller; the **Data Protection Officer (DPO)**, i.e. the official responsible in each institution for

ensuring the internal application of the 2001 provisions; the **Data Protection Coordinator** (DPC), the person appointed by the director-general (or similar) to check the correct implementation of DPO instructions; and the **European Data Protection Supervisor** (EDPS), the independent supervisory authority that ensures the application of the rules across all the EU institutions. This latter is established by Regulation 45/2001, which specifies the powers and duties.

Regulation 45/2001 sets out the **EDPS's** tasks, in particular in terms of:

supervision and **enforcement** (by monitoring the application of the rules stated in the regulation, including through prior checks and keeping a register of notified data processing; by investigating complaints lodged by data-subjects and conducting inspections at EU institutions and bodies on his or her own initiative, or based on a complaint);

consultation (by, for example, advising data-subjects, controllers and the EU institutions, the latter also on legislative and administrative measures on data protection matters,⁴ and appearing before the CJEU); **cooperation** (with data protection authorities and other bodies). The EDPS also monitors the development of technologies and provides guidelines on them.

Rules and obligations

Data controllers within the EU institutions have, like other controllers, the obligation to **inform** the data-subject; to maintain accurate and updated data; to pay special attention to **sensitive** data (e.g. ethnic origin, political opinions, religious beliefs, trade union membership, health and sex life); to **delete** or block data if no longer needed for the original purpose; to make data accessible to the data-subject; to ensure the technical and organisational security of personal data; to respond (usually within 15 days) to a data-subject's requests regarding the exercise of their **rights**, e.g. the right to access, rectification, blocking, erasure, and to object to processing of personal data.⁵

Moreover, the regulation provides for the mandatory appointment of a **DPO** within each EU institution, to ensure that the rules are applied and to advise data controllers.

A general **notification** procedure is required, meaning that the data controller has to contact and inform the DPO prior to undertaking a processing operation: the DPO keeps a register of data processing and has to consult the EDPS through the system of **prior checks** when processing operations are likely to present risks to subjects' rights.⁶

Finally, any failure to comply with the obligations provided in Regulation 45/2001 may make any civil servant of the EU institutions liable to **disciplinary action** (according to the Staff Regulations of officials of the EU institutions).

Parliament's starting position

The European Parliament (EP) has called for a consistent legal framework on data protection on several occasions, for instance in its resolutions of 2011 [on a comprehensive approach on data protection](#), of 2016, '[towards a digital single market act](#)', and of 2017 on [Fundamental rights implications of big data](#).⁷

European Council starting position

In its December 2015 conclusions, the European Council invited the EU institutions to accelerate implementation of the digital single market strategy, and welcomed the agreement on the data protection package as a major step forward. In its June 2017 [conclusions](#) and March 2018 [conclusions](#) it highlighted the importance of an ambitious digital vision for Europe, which requires the implementation of the DSM strategy in all its elements, including data protection.

Preparation of the proposal

According to the [GDPR](#) (Article 98), the European Commission must adapt Union legal acts applicable to the processing of personal data by the Union institutions and bodies in line with the new rules, in particular Regulation (EC) No 45/2001.

Evaluation study

In the context of the reform of the data protection legal framework, the European Commission published the results of an **evaluation study** on the current Regulation 45/2001 in 2015, including an assessment of its application and efficiency.⁸ From this study it emerged that, while safeguards for data protection across EU institutions are adequately established and implemented, some aspects of Regulation 45/2001 need to be improved or changed. The need to provide Data Protection Officers (DPOs) with greater support and to enhance the EDPS's powers also emerged. Another conclusion was that data controllers within the EU bodies should perform risk assessments in order to implement data protection requirements more effectively. Attention was also drawn to the need to **simplify** the notifications regime and prior checks on data processing so as to reduce the administrative burden: these are considered time consuming for the EDPS and for the DPOs in charge of drafting the notification to the EDPS.

The study deemed the norms on data protection in telecommunications networks to be outdated in the light of the e-Privacy Directive (also to be replaced by the proposed e-Privacy regulation). The study also noted that the system of remedies and sanctions is appropriate but not necessarily applied. The EU Court of Justice (CJEU) has ruled on the application of Regulation 45/2001 in a [few cases](#) including on the balance between the right to access to documents and data protection. As for the free flow of data, the study recommended that the reform of Regulation 45/2001 clarifies the rules related to data transfer, as their implementation has raised difficulties that hindered their effectiveness. Other recommendations included: increasing the EDPS resources dedicated to inspections in view of the increase in accountability (as provided for by GDPR).

Information on the application of the current Regulation 45/2001 within the EU bodies was also gathered from an EDPS survey.⁹

The Commission considered it unnecessary to carry out an impact assessment on data protection rules for EU institutions as the proposal is to be aligned with the GDPR and the impact of the new obligations has been assessed in the context of the preparatory work on the latter. In this case, the impact will fall mainly on EU institutions and agencies.¹⁰

EPRS impact assessment

An assessment of some aspects of the impact of the new proposal was carried out by EPRS in 2017 upon request of the Civil Liberties, Justice & Home Affairs (LIBE) Committee. The [EPRS study](#),¹¹ taking the new obligations for data controllers and DPOs into account, focused on three specific aspects: the impact of the new model of governance and accountability of the proposal on the Union institutions and bodies; the implication of this measure in terms of budget and human resources; and the possible risks deriving from a decentralised model in terms of consistency and uniform application of the regulation.

The main findings of the EPRS study suggest that there will be an increase in workload for data controllers and DPOs, although this impact would be limited to the initial period of application only (expected to be 1-2 years). In terms of human resources and related costs, this study notes that DPOs will be heavily impacted (with a potential high increase

in workload and therefore in costs). However, factors that may limit the impact of the new regulation are also considered, such as stakeholder capacity to adapt, IT-tool-related efficiency gains, and better management of data protection activities. The risks, in terms of uniform application of the rules, generated by the decentralised model proposed by the reform, may include the possibility of several controllers within the same institution, and difficulties for DPOs to obtain adequate information. This, however, could be mitigated by a clear distribution of roles and responsibilities, by the new DPO's role more oriented toward advice activities and by the strengthening of the EDPS supervision role.

EDPS study

A [survey](#) published by the EDPS on the state of play of compliance of the EU institutions with current data protection rules (based on the responses of 64 EU bodies) confirmed a positive trend among EU institutions processing data in their administrative duties. Accordingly, adapting to the new rules will be easier for the well-established institutions. For others, EDPS will provide 'the necessary support to ensure that data protection becomes a reflex'. Challenges have been identified in the increasing international data transfers and in ad hoc training needs.

The changes the proposal would bring

The reform's goal is to produce a coherent and up-to-date framework on the processing of data by EU institutions, capable of striking a balance between ensuring free movement of data and services within the EU and individuals' rights.

A new regulation

The Commission proposed a new [regulation](#) to replace the 2001 provisions, in order to align them with those laid down in the GDPR, in particular by providing individuals with stronger legally enforceable rights, specifying the obligations of data controllers in the EU institutions, and strengthening the role of the EDPS.

Scope

The proposed regulation would apply to data processing by automated means or otherwise, if part of a filing system, by Union institutions and bodies, including the transfer of data between them (or to recipients established in the Union and subject to the GDPR). The original proposal included the condition 'insofar as such processing is carried out in the exercise of activities which fall within the scope of Union law.

The proposed regulation contains a Chapter VIIIa with general rules on processing of *operational personal data* by Union agencies, offices and bodies when carrying out activities in the field of judicial and police cooperation: this without prejudice to specific data protection provisions contained in their founding acts (*lex specialis*). The draft regulation (Article 2) would not apply to the processing of *operational* personal data by Europol and the European Public Prosecutor's Office, until the respective acts (Regulations No 2016/794 and No 2017/1939) are adapted, nor to missions.

Definitions

While some of the proposal's definitions are specific to this regulation (e.g. that of *controller*, *user*, *operational data* or *directory*), others are identical to the GDPR (e.g. that of consent, processing, profiling, etc).

Regarding its own definition of data **controller**, unlike the GDPR, the proposed regulation does not include the reference to *natural* persons. Accordingly a controller is: a Union institution, body, office or agency or the directorate-general or any other organisational entity which determines, also **jointly**, the purposes and means of the processing of personal data), the new definition does not include '*unit*' (this term was used in

Regulation 45/2001), but it may be included if considered as an 'organisational entity'.¹² Also 'controllers *other than* Union institutions' (relevant for data transfers outside the EU institutions) means controllers within the meaning of Article 4(7) GDPR, i.e. *any natural or legal person, public authority, or other body determining the purposes of data processing*.

Each controller must maintain a **record** of processing activities under its responsibility. The data processor, is, rather, defined as 'the natural or legal person or public body processing data on behalf of the controller'.

Main principles and rules

Data must be processed according to the principles of lawfulness and fairness, purpose limitation,¹³ data minimisation and accuracy (Article 4). Changes introduced with the reform include increased transparency and accountability principles, in line with the GDPR. The criteria for **lawful** data processing are similar to those of the GDPR (consent, necessity to perform a task in the public interest, or in the exercise of official authority vested in the Union body, *or in compliance with a legal obligation*, laid down in a Union act) with the exception of the controller's legitimate interest, which is not applicable to the public sector and thus to the Union institutions (Article 5).¹⁴

Under some conditions, data processing is possible for **other compatible purposes** than that for which data were initially collected (Art 6).

In line with the GDPR, **consent**, to be valid as legal grounds, must be freely given and unambiguous, expressed by a clear affirmative act (including ticking a box).¹⁵ Processing data for the same purposes for which the institution, as controller, has already got the subject's consent does not require new consent, as far as the controller can demonstrate that a clear indication of consent was obtained in the past.

According to the principle of **accountability**,¹⁶ the EU institution as controller needs to be able to *demonstrate* compliance with the regulation.¹⁷ Transmission of data to recipients, other than Union bodies may take place under some conditions (Article 9), e.g. when it is necessary for the performance of a task carried out in the public interest.

In view of strengthening individuals' rights, the proposed regulation strengthens **obligations** on controllers (Art 14-16), such as to provide transparent, easily accessible **information** (including icons) as well as mechanisms for exercising the individual's rights (including making electronic requests). Information must include the storage period, the right to lodge a complaint and on possible international transfers. Exceptions apply, e.g. if personal data must remain subject to an obligation of professional secrecy regulated by EU law (e.g. data processed by services competent for social security or health matters).

The subject's **rights** include the right to access (to data concerning the individual and processed by the institutions), the right to rectification and to erasure ('right to be forgotten'), as well as the right to obtain restrictions to processing in certain cases (former 'right to blocking') from the controller, the right to data portability (transmit data to another controller), and the 'right to object' to certain data processing.

According to the proposed regulation, **restrictions** to these rights – which are necessary and proportionate, to safeguard, for example, national security, public security, the prevention of or investigation of crimes, the internal security of the institutions, or another important general public interest of the Union or of a Member State, such as common foreign and security policy, and which respect the *essence* of fundamental rights¹⁸ – may be provided by a legal act on the basis of the Treaties or **by the internal**

rules of Union institutions in matters relating to the *operation* of the institutions. The proposed regulation (Article 25) allows, in matters relating to the operation of the Union institutions, for internal rules as a basis for restrictions of rights, but (in compliance with Article 52(1) CFR) providing they are **clear and precise** acts of general application, intended to produce legal effects vis-à-vis data-subjects, adopted at the highest level of management of the institutions, subject to publication in the Official Journal and containing specific provisions.

Regarding **special categories** of data (e.g. on health, or religious or political opinion), derogations from the general prohibition to process them (Article 10) include: processing is necessary in the field of employment and social security and authorised by law or is carried out by a non-profit-making body which constitutes an *entity integrated in a Union institution* and with a *political*, philosophical, religious or trade-union aim or if processing relates to data that are manifestly made *public* by the data-subject.

Another novelty, in line with the GDPR, is the right of the subject to object to data processing, although necessary for a task carried out in the public interest (including profiling), and not to be subject to a *solely* automated decision (i.e. a decision affecting an individual based solely on automated processing, without human intervention), for instance for e-recruitment. Also, the principles of **data protection by design** (the system of data processing is designed from the beginning to minimise the collection of data and to use, for instance, pseudonymisation) and **by default** (only necessary data should be processed), are now extended to the Union institutions.

Enforcement and control

A data protection **impact assessment** (Article 39) must be conducted by a controller prior to data-processing operations that might result in high risks to the rights of individuals (e.g. if using new technologies for evaluation of personal aspects of persons based on profiling). If data processing results in high risks, and in the absence of appropriate safeguards and security measures, consultation with the EDPS is mandatory.

The position of the **DPO** (Articles 44-46), who is a staff member designated by each institution, is also strengthened and the EU institutions must ensure that they are involved in all issues that relate to data protection. The DPO's tasks include: informing and advising the controller; ensuring in an independent manner the internal application of the regulation, and monitoring compliance with it and other data protection policies.

As the current Regulation No 45/2001 defines the powers and duties of the **EDPS**, the draft regulation contains several provisions (Chapter VI) aimed at strengthening these powers and redefining duties.¹⁹ The EDPS recently also became the supervisory authority for Europol, and coordination with national supervisory authorities is encouraged. While the new regulation confirms, inter alia, the EDPS's task of **monitoring and enforcing** the application of this regulation by a Union institution or body, with the exception of data processing by the CJEU acting in its judicial capacity, it also clarifies the EDPS's investigative powers (Article 59).²⁰

New rules are provided for the **transmission** of personal data to recipients other than Union institutions and bodies (such as private entities). Recipients should demonstrate that it is necessary to have the data transmitted to them either for the performance of their task carried out in the public interest or in the exercise of official authority vested in them (Recital 22).

Transfers outside the EU may take place on the basis of a European Commission adequacy decision (e.g. [EU-US Privacy Shield](#)), or of adequate safeguards, such as standard contractual clauses or binding corporate rules.

Regarding the regime of **remedies**, the proposal confirms the right of any data-subject to lodge a complaint with the EDPS, and the right to compensation, for both material and non-material damage. Tougher **sanctions** are provided in cases of infringement, and the EDPS has the power to impose **administrative fines** on Union institutions and bodies as a last resort and only where the institution has failed to comply with an order by the EDPS.²¹

Attention is paid also to the confidentiality of electronic communications to be secured by the Union institutions, in particular by securing their electronic communications networks (new Section 2A). The draft regulation also protects data relating to the terminal equipment of end-users accessing publicly available websites and mobile applications offered by Union institutions, in accordance with the current e-Privacy Directive and in view of the upcoming [e-Privacy regulation](#).

Finally, security of data processing should be ensured. Adherence to an approved certification mechanism (as in Article 42 GDPR) may be used to demonstrate compliance with the security requirements (technical and organisational measures, Article 33).

Advisory committees and other bodies

European Economic and Social Committee (EESC)

The European Economic and Social Committee (EESC) adopted its [opinion](#) on the draft regulation in May 2017 (rapporteur: Jorge Pegado Liz, Various interests – Group III, Portugal). The EESC generally welcomed the initiative and its innovations (e.g. the introduction of explicit administrative fines for infringements) and suggested some amendments.

Article 29 Data Protection Working Party

The independent European advisory body on data protection, the Article 29 Working Party (Art29WP), representing the European data protection authorities (DPAs) and set up under Article 29 of Directive 95/46/EC, published a [statement](#) in April 2017 regarding the current reform. It underlined therein the importance of ensuring consistency with the GDPR, in particular concerning the requirement that possible restrictions to the rights of data-subjects have to be provided **by law**.

European Data Protection Supervisor (EDPS)

The EDPS, as mentioned above, was established by Regulation 45/2001, and accordingly has, among others, the duty of advising on legislative acts.²² In March 2017, the EDPS released an [opinion](#) on the proposal.²³ The EDPS position was mainly in line with that of Art29WP. The EDPS emphasised that, from the perspective of the individual, it is essential that the principles are applied consistently throughout the EU, irrespective of who is the data controller, and in line with the GDPR.

National parliaments

A number of [national parliaments](#) have examined the proposal, without raising objections. Contributions from some chambers (Portuguese Parliament, Czech Chamber of Deputies, Spanish Cortes Generales) were received by end-May 2017.

Stakeholders' views²⁴

While stakeholder positions (i.e. mainly from EU bodies) on the proposal may be said to be convergent on the main principles, some crucial aspects were controversial as they emerged also from the EPRS impact assessment study²⁵.

[Eurojust's position](#) is that both the revised Regulation 45/2001 and [Eurojust Regulation](#) should create no obstacles to operational work, offering legal certainty *in specie* to the

national authorities that entrust data on investigations to Eurojust: in particular, it was in favour of a *lex generalis – lex specialis* approach, where the special rules of Eurojust (e.g. limitation to individual rights) would prevail in case of conflict with the new regulation. Similar considerations have been expressed by [Europol](#).

The [EDPS](#), a key player in the implementation of the new rules, has advocated uniformity of the data protection legal framework, while accepting the uniqueness of the EU public sector. The [EDPS](#) has stressed the importance of the new regulation for all EU institutions as 'a statement of the EU's commitment to subject itself to the same rules that will apply to others under the GDPR and the law enforcement directive', in this way excluding special treatment for the 'EU bubble'. The [EDPS](#) also urged the co-legislators to avoid further delay in the adoption of the new regulation.

Legislative process

The [legislative proposal \(COM\(2017\) 8\)](#) was published on 10 January 2017.

Parliament

Within the European Parliament, the proposal was assigned to the Civil Liberties Committee (LIBE). The [report](#) (rapporteur: Cornelia Ernst, GUE/NGL, Germany), put forward several [amendments](#),²⁶ aimed at harmonising the data protection regime for EU bodies carrying out activities relevant in the area of *judicial cooperation in criminal matters* and *police cooperation*: i.e. Eurojust, Europol, and the European Public Prosecutor's Office, as well as missions (referred to in Articles 42-44 TEU, which implement the common security and defence policy, CSDP). Also, the indication of internal rules as ground for restrictions of data protection rights was deleted from the proposal. The LIBE committee adopted its report and the mandate to enter into interinstitutional negotiations in October 2017.

The Committee of Legal Affairs (JURI) adopted its [opinion](#) on 2 September 2017, while the Committee on Budgets (BUDG) decided not to give an opinion.

Council of the EU

The Council meanwhile had adopted its [general approach](#) in June 2017. In particular, it aimed to exclude from the scope of the regulation the processing of 'operational personal data', such as data processed for criminal investigations by EU bodies like Europol and Eurojust (at least when the establishing acts of these bodies provide for comprehensive data protection rules²⁷), and data processing by CSDP 'missions'.

Trilogue negotiations

[Trilogue](#) negotiations on the file advanced under the Estonian and Bulgarian Presidencies. The main issue at stake was the scope of the regulation and thus setting specific requirements for operational data of the EU's justice and home affairs agencies while keeping a harmonised framework. The European Parliament's rapporteur insisted on the inclusion within the regulation of an additional chapter on operational data (*Chapter VIIIa*).²⁸

At the end of February 2018, the EP noted that there had been insufficient progress due to lack of convergence between the positions of the two co-legislators.

In March, the Council Presidency presented a redrafted [compromise text](#) concerning the scope of the regulation: although it was open to a dedicated 'operational data' chapter, it recognised the prevalence of specific rules *applicable* to those Union bodies, offices or agencies that provide otherwise (*lex specialis*) over such a chapter. The reliance on internal rules as grounds for restricting data protection rights was another of the issues raised during the trilogues.

A [compromise](#) between the co-legislators was reached in May 2018 (two days before the 25 May deadline of the GDPR's full application), and subsequently endorsed by the LIBE committee in July. It is due be discussed and voted by the EP during the September plenary session, and would thereafter be formally adopted by the Council.

The agreed text includes a new chapter on operational data processed by EU bodies and agencies carrying out law enforcement activities, without prejudice to their prevailing specific data protection norms. (It may be noted that [Declaration No 21 accompanying the Lisbon Treaty](#) recognises the necessity for specific rules on the protection of personal data in the fields of judicial and police cooperation, as is the case for the [Law Enforcement Directive](#).) A key aim of the new regulation is to provide a coherent approach on data protection in this area too.

EP supporting analysis

['Assessment of the impact of specific aspects of the new model of governance and accountability of data protection by Union institutions and bodies proposed by the Commission'](#), substitute impact assessment, EPRS, October 2017.

[Data protection rules applicable to the European Parliament and to MEPs](#), Briefing, EPRS, June 2018.

Other sources

[Protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and the free movement of such data](#), European Parliament, Legislative Observatory (OEL).

European Data Protection Supervisor, [Opinion 3/2015 'Europe's big opportunity: EDPS recommendations on the EU's options for data protection reform'](#).

Endnotes

- ¹ EPRS, [Data protection reform package](#): Final steps, 2016. The 1995 directive was complemented by the e-Privacy Directive ([Directive 2002/58/EC](#)) as regards the confidentiality of e-communications, still in force.
- ² Article 16 TFEU recognises the right to data protection for any individual, and provides that the rules adopted by the EU and Member States acting within the scope of EU law and related to the protection of individuals with regard to data processing are to be laid down following the ordinary legislative procedure.
- ³ European Commission [proposal](#) for a regulation on data protection in EU institutions, explanatory memorandum.
- ⁴ A '[policy toolkit](#), assessing the necessity of measures that interfere with fundamental rights' has been provided by EDPS containing general guidance to the legislator. Each year the EDPS makes a list of the policy initiatives planned by the European Commission in its work programme that will require advice or monitoring.
- ⁵ See for instance the [Guide for users](#) prepared by the EP on the basis of Regulation 45/2001 and the website [legal notice](#).
- ⁶ If personal data are handled by a processor that is a contractor, the data controller must ensure the contractor applies the same data protection measures, as defined in the legal agreement between the contractor and the institution concerned.
- ⁷ See also the [event](#) organised by the EP Data Protection Service, 'A New Chapter for EU Data Protection: Managing accountability and compliance'.
- ⁸ See European Commission, [Evaluation Study on Regulation \(EC\) 45/2001 \(by Ernst and Young\)](#).
- ⁹ EDPS, 'Measuring compliance with Regulation (EC) 45/2001 in EU institutions' ('[Survey 2013](#)').
- ¹⁰ See European Commission [proposal](#) for a regulation on data protection in EU institutions, explanatory memorandum.
- ¹¹ For the purpose of the study, a survey was conducted among different stakeholders (data controllers, DPOs) within the main EU institutions, including the European Commission, European Parliament, OLAF and EEAS.

- ¹² On its application to the European Parliament and MEPs, see EPRS Briefing, [Data protection rules applicable to the European Parliament and to MEPs](#), June 2918; See also EP Data Protection Service, Recommendation 2/2018 on the data protection rules applicable to contracts between the EP and private companies.
- ¹³ Further processing for archiving purposes in the public interest, scientific, research or statistical purposes shall not be considered to be incompatible with the initial purposes (Article 4).
- ¹⁴ However, see Article 23 of the proposal where compelling legitimate grounds of the institution, over-riding individuals' rights, once demonstrated, can restrict the right to object.
- ¹⁵ When assessing if the consent is freely given, it should be taken into account whether the performance of a contract, including the provision of a service, is conditional on consent to the processing of data that is not necessary for the performance of that contract.
- ¹⁶ See, inter alia, [EDPS](#) provisional guidance on accountability.
- ¹⁷ This includes the adoption of appropriate technical and organisational measures and, where appropriate, *internal policies* and mechanisms for ensuring such compliance.
- ¹⁸ On the problematic definition of this concept see, inter alia, M. Brkan, [In Search of the Concept of Essence of EU Fundamental Rights through the Prism of Data Privacy](#) Maastricht Faculty of Law Working Paper, No 2017-01.
- ¹⁹ The new regulation will also repeal [Decision No 1247/2002/EC](#) governing the EDPS's duties.
- ²⁰ These include: to carry out investigations in the form of data protection audits; to obtain, from the controller access to all personal data and information necessary for its tasks; to obtain access to *any premises of the controller*, including to any data processing equipment and means, in accordance with Union law.
- ²¹ The EDPS adopted practical guidelines in early 2018 to help EU institutions processing personal data, taking into account the GDPR, which provide recommendations on implementing accountability for data protection by outlining the approach the institutions should take in the development and [maintenance of information systems](#) and databases (including 'privacy by design') as well as when opting to [process data using cloud-based services](#).
- ²² See also EDPS, [Priorities for providing advice in 2017](#), note of 15 February 2017.
- ²³ EDPS, Summary of [Opinion](#) of 24 May 2017.
- ²⁴ This section aims to provide a flavour of the debate and is not intended to be an exhaustive account of all the different views on the proposal. Additional information can be found in related publications listed under 'EP supporting analysis'.
- ²⁵ While, for instance, the Commission supports the idea that the general workload will not see major changes, stakeholders interviewed for the EPRS study hold a different view.
- ²⁶ As regards the legal grounds for data processing (Article 5) necessary to perform a task, it was clarified that this task shall be laid down in Union law. The committee's report suggested also making reference to Member State law to which the controller is subject.
- ²⁷ See for instance [Eurojust Rules](#) on the processing of personal data at Eurojust.
- ²⁸ See also Council, [compilation](#) of Member States written contributions, 16 February 2018.

Disclaimer and Copyright

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.

© European Union, 2018.

eprs@ep.europa.eu

<http://www.eprs.ep.parl.union.eu> (intranet)

<http://www.europarl.europa.eu/thinktank> (internet)

<http://epthinktank.eu> (blog)



Third edition. The 'EU Legislation in Progress' briefings are updated at key stages throughout the legislative procedure.