guide to the revised data protection regulation (ec)[[1]](#footnote-1)

Version 2.0 of 11/12/2018

Mariya KOLEVA



Contents

[1. Introduction 4](#_Toc524354223)

[2. The proposal at glance 4](#_Toc524354224)

[3. Concepts and definitions 5](#_Toc524354225)

[3.1. Principles 5](#_Toc524354226)

[3.2. Processing for another compatible purpose (Article 6) 5](#_Toc524354227)

[3.3. Special categories of data (Article 10) 6](#_Toc524354228)

[3.4. Joint controllership (Article 28) 6](#_Toc524354229)

[4. Improved right for data subjects 6](#_Toc524354230)

[4.1. Transparency (Article 14) 6](#_Toc524354231)

[4.2. Right to erasure (‘Right to be forgotten’) (Article 19) 6](#_Toc524354232)

[4.3. Right to restrict the processing of personal data (Articles 20) 7](#_Toc524354233)

[4.4. Right to data portability (Article 22 7](#_Toc524354234)

[4.5. Right to withdraw consent at any time [Article 7(3)] 7](#_Toc524354235)

[4.6. Right to lodge a complaint with the EDPS (Article 63 et seq.) 8](#_Toc524354236)

[4.7. Restriction of rights (Article 25) 8](#_Toc524354237)

[5. Controllers’ obligations 8](#_Toc524354238)

[5.1. Data subject’s consent (Article 7) 8](#_Toc524354239)

[5.2. Data protection by design and by default (Article 27) 8](#_Toc524354240)

[5.3. Data protection impact assessment (Article 39 et seq.) 8](#_Toc524354241)

[5.4. Obligation to notify the EDPS and the data subject of a data breach (Articles 37 and 38) 9](#_Toc524354242)

[5.5. Security of personal data and confidentiality of communications (Articles 33 and 38a) 9](#_Toc524354243)

[5.6. Protection of directories of users (Article 38b) 9](#_Toc524354244)

[6. Clarification of processors’ obligations 9](#_Toc524354245)

[7. Simplification of procedures 10](#_Toc524354246)

[7.1. Transfer of data within or between institutions 10](#_Toc524354247)

[7.2. Prior consultation of the EDPS (Article 40) 10](#_Toc524354248)

[7.3. Records of processing activities (Article 31) 10](#_Toc524354249)

[8. Fines for non-compliance with data protection rules 10](#_Toc524354250)

[8.1. [Articles 66 and 29(10)] 10](#_Toc524354251)

[9. Other provisions 11](#_Toc524354252)

[9.1. Data protection officer (Articles 44-46) 11](#_Toc524354253)

[9.2. International data transfers (Article 47-52) 11](#_Toc524354254)

[9.3. Specific provisions for archiving (Article 13) 11](#_Toc524354255)

# Introduction

The protection of personal data is a fundamental right enshrined in Article 8 of the Charter of Fundamental Rights of the European Union (Charter). However, the right to personal data protection is not an absolute right and it may be limited if nec­essary for an objective of general interest or to protect the rights and freedoms of others. This fundamental right has to be understood in conjunction with the right to respect for private and family life of Article 7 of the “Charter” and Article 8 of the European Convention of Human Rights (ECHR).

The General Data Protection Regulation[[2]](#footnote-2) (GDPR) became directly applicable to the Member States on 25 May 2018. It strengthened the enforcement of the EU of people´s fundamental right to data protection. It introduced a risk-based approach to assessing data processing operations and put data protection compliance at the centre of organisations´ governance.

In order to ensure a coherent and harmonised approach to data protection throughout the Union, EU Institutions´ and bodies´ data protection rules (Regulation (EC) 45/2001[[3]](#footnote-3)) have been aligned with the new arrangements. As a result, future data processing operations will be subject to higher standards of compliance. The EU Commission adopted on 23 October 2018 the new Regulation (EU) No 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (the ‘EU Data Protection Regulation’). These rules enter into force on 11 December 2018.

This Guide is based on the text of the revised Regulation and on the EU Commission Guide to the Commission proposal for the revision of Regulation (EC) 45/2001. It is designed to assist the CPVO staff prepare the adjustments of internal procedures and practices that will be necessary under the new data protection rules.

Please note that this is not an exhaustive guide: it presents the main changes to internal data protection rules and briefly summarises other relevant elements. The Data Protection Office intends to provide more detailed and comprehensive information.

# The new Regulation at glance

* The new Regulation No 2018/1725 does not change the substance of the legal framework governing the processing of personal data by the EU institutions and bodies; rather, it clarifies and strengthens key concepts and principles.
* In addition to introducing a risk-based approach, it places greater emphasis on transparency and **accountability[[4]](#footnote-4)**.
* It uses new concepts such as **data protection by design** and **by default[[5]](#footnote-5)**.
* The following rights of data subjects are improved or clarified:
* the ´***right to be forgotten***´; and
* the ***right to data portability***.

Also, in some cases, the use of their data is subject to their explicit, specific and revocable consent.

* **New obligations** require controllers to carry out data protection impact assessments (DPIAs), to notify personal data breaches to the EU Data Protection Supervisor (EDPS) and to the data subjects, and to document processing activities. On the other hand, administrative burden is lessened by the removal of the obligations to notify the DPO and carry out prior check procedure.
* The EDPS can impose **administrative fines**.
* The **DPO** is tasked with monitoring institutions´ compliance with the Regulation and with their internal policies.
* The EDPS´s powers, in terms of supervision, enforcement and legislative consultation, remain broadly unchanged.

# Concepts and definitions

The new Regulation uses the same definitions as the GDPR and the e-Privacy Regulation[[6]](#footnote-6) . New elements are as follows:

## Principles

The new Regulation No 2018/1725 lists in a more systematic way the principles relating to the processing of personal data:

* lawfulness, fairness and transparency;
* purpose limitation;
* data minimisation;
* accuracy;
* storage limitation;
* integrity and confidentiality; and
* accountability.

## Processing for another compatible purpose (Article 6)

The processing of personal data for purposes other than originals ones can be foreseen as long as the new purpose is compatible with the purposes for which the personal data were initially collected. This dimension of the purpose limitation principle may avoid the need of an additional legal basis separate from that which allowed the original collection of the personal data. Considering a new purpose compatible with the original purpose requires a close to look at:

* Any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
* the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
* the nature of the personal data,
* the possible consequences of the intended further processing for data subjects;
* the existence of appropriate safeguards, which may include encryption or pseudonymisation.

## Special categories of data (Article 10)

The definition of ´special categories´ of data (data revealing: racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership and data concerning health) is extended to genetic or biometric data used to identify a natural person, and data concerning a person´s sex life and sexual orientation.

The rule on the processing of special category remains the same: it is prohibited except in certain clearly defined circumstances. However, the proposal does add new exceptions – such data can be processed:

* When necessary for reasons of public interest in the area of public health;
* For archiving purposes in the public interest; and
* In order for health professionals to assess and employee´s capacity to work (subject to the obligation of professional secrecy).

## Joint controllership (Article 28)

The definition of ´controller´ in the old Regulation (EC) 45/2001 already allowed for joint controllership, but the new rules include separate article on this, defining it as a situation where a ´a Union institutions or body together with one or more controllers or controllers, which may be or not be Union institutions and bodies, jointly determine the purposes and means of the processing´. Joint controllers must establish their roles and respective responsibilities in a transparent manner in the light of their data protection obligations. They have to design a contact point for data subjects and give them access to information on the essential points of the arrangements in place.

# Improved right for data subjects

## Transparency (Article 14)

The controller must help data subjects to exercise their rights by facilitating access to information and presenting it in clear, plain language. In practice, this means that privacy and data protection notices and statements must be more readily available and drafted concisely, transparently and intelligibly.

## Right to erasure (‘Right to be forgotten’) (Article 19)

A person can request erasure of his/her personal data if:

* it is no longer necessary for the purpose for which it was collected;
* he/she objects to, or withdraws consent for, its processing; or
* the processing has been unlawful.

This right is not absolute – it has to be balanced case by case against other rights (e.g. freedom of expression), public interest in the area of public health and the need for archiving in the public interest.

The controller must take reasonable steps, including technical measures, to inform other persons/organisations processing the data, such as search engines, that the data subject has requested erasure of links, copies or replications of the data. In each case, the definition of ‘reasonable steps’ will depend on what technology is available and the cost of implementation

## Right to restrict the processing of personal data (Article 20)

A person can ask the controller to restrict the processing of his/her personal data under certain circumstances. This is the equivalent of the right of ‘blocking’ in the old Regulation (EC) No 45/2001.

The data subject has the right to obtain from the controller restriction of processing of his/her data where one of the following applies:

* the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy, including the completeness, of the personal data;
* the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
* the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
* the data subject has objected to processing pursuant to Article 23(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

It is worth to be reminded that ‘restriction of processing’ means the marking of stored personal data with the aim of limiting their processing in the future. The data cannot be deleted while it is ´restricted´. Where processing has been restricted, personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

## Right to data portability (Article 22)

A person is entitled to ask a controller to give him or her personal data which he or she has provided, in a structured, commonly used and machine-readable format, and to transmit those data to another controller. Where technically possible, the controller has to transmit the data directly itself.

The right to data portability is applicable where the processing is:

* based on consent or on a contract; and
* carried out by automated means.

In exercising this right, the data subject has the right to have the personal data transmitted directly from one controller to another or to controllers other than Union institutions and bodies, where technically feasible.

## Right to withdraw consent at any time (Article 7(3))

Where applicable the controller must ask for consent in clear, plain language and inform data subjects of their right to withdraw their consent at any time. It should be as easy to withdraw consent as to give it.

The withdrawal of consent has no bearing on the lawfulness of any previous processing based on consent before its withdrawal.

## Right to lodge a complaint with the EDPS (Article 63 et seq.)

Under the old Regulation (EC) No 45/2001, data subjects could lodge a complaint with the EDPS, which had to hear and investigate it and inform them of the outcome within a reasonable period. The new Regulation No 2018/1725 enshrines this right and requires the EDPS to handle the complaint or inform the data subject within three months; failing this, the complaint is deemed to have been rejected

## Restriction of rights (Article 25)

The proposal allows data subjects’ rights to be restricted only on the basis of:

* a legal act based on the Treaties; or
* (for matters relating to the operation of Union institutions and bodies) internal rules.

If the restriction is based on internal rules, those should be clear and precise acts of general application, intended to produce legal effects vis-a-vis data subjects, adopted at the highest level of management of the Union institutions and bodies and subject to publication in the Official Journal of the European Union.

The right not to be subject to automated decision making cannot be restricted under any circumstances, while the right to object can be restricted only for scientific, historical research or statistical purposes or for the purposes of archiving in the public interest.

Where a restriction is imposed on the basis of Union law, the data subject shall be informed of the principal reasons and of his or her right to lodge a complaint with the EDPS.

‘Restrictions’ in the new Regulation No 2018/1725 are equivalent to ‘exemptions’ in Regulation (EC) No 45/2001.

# Controllers’ obligations

## Data subject’s consent (Article 7)

The new Regulation No 2018/1725 clarifies that consent is a valid basis for lawful processing where the controller:

* can demonstrate that the data subject has consented to the processing of his/her data; and
* has asked in advance for consent in clear, plain language, and separately for each type of data processing activity (no ‘bundle consent’).

Consent must be given by a clear, affirmative act indicating the data subject’s freely given, specific, informed and unambiguous agreement: silence, inactivity or pre-ticked boxes do not constitute valid consent.

## Data protection by design and by default (Article 27)

The new Regulation No 2018/1725 introduces the concept of data protection by design and by default. In concrete terms, this means that the controller must take appropriate technical and organisational measures to ensure that data protection is integral to the processing operation and that personal data is processed only to the extent necessary for each specific purpose of the processing.

The appropriate technical and organisational measures should be implemented by the controller, both at the time of the determination of the means for processing and at the time of the processing itself, in an effective manner and so to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

## Data protection impact assessment (Article 39 et seq.)

If the processing of personal data is likely to result in a high risk to the rights and freedoms of individuals, the controller must first carry out a DPIA.

The DPIA describes the processing operation and its purposes, the risks to the rights and freedoms of individuals and specific measures envisaged to address the risks.

In particular, a DPIA will be required in the event of:

• systematic and extensive evaluation of personal data based on automatic processing (including profiling) and leading to decisions producing legal effects;

• large scale processing of special categories of data; and

• large scale systematic monitoring of publicly accessible areas.

The EDPS will draw up a list of the kind of processing operations that will require a DPIA.

## Obligation to notify the EDPS and the data subject of a data breach (Articles 34 and 35)

In the event of a personal data breach, the controller must notify the EDPS without undue delay and, where feasible, no later than 72 hours after becoming aware of it, unless it is unlikely to result in a risk to the rights and freedoms of natural persons. The controller must also inform the DPO.

The controller must document the circumstances of the breach, its impact and remedial action taken to enable the EDPS to verify compliance with these provisions.

The controller must also notify the data subject if the breach is likely to result in a high risk to the rights and freedoms of natural persons. The notification must be in clear, plain language and contain at least the DPO’s name and contact details, an indication of the likely consequences of the breach and a description of measures taken by the controller.

The controller does not have to notify the data subject where: 1. it has taken technical and organisational measures (e.g. encryption) that render the data unintelligible to unauthorised persons. 2. it takes measures that render the risk no longer likely to materialise, and 3. it means a disproportioned effort.

## Security of personal data and confidentiality of communications (Articles 33 and 36)

The new Regulation No 2018/1725 goes into greater detail than Regulation (EC) No 45/2001 in describing the security measures that the controller must take, e.g. pseudonymisation and encryption.

It also emphasises EU institutions’ and bodies’ obligation to ensure the confidentiality of electronic communications by securing their networks.

## Protection of directories of users (Article 38)

As regards the protection of information in end-users’ equipment, the new Regulation No 2018/1725 contains the same rules as the proposal for ePrivacy Regulation.

The new Regulation No 2018/1725 requires that personal data in user directories be limited to what is strictly necessary and that directories be protected from being used for marketing purposes.

# Clarification of processors’ obligations

The new Regulation No 2018/1725 clarifies processors’ obligations, in particular strictly regulating the extent to which they can take on other processors to carry out specific processing activities on behalf of the controller.

Subcontracting to other processors is subject to prior written authorisation by the controller.

# Simplification of procedures

## Transfer of data within or between institutions

Unlike Regulation (EC) No 45/2001, the new Regulation No 2018/1725 contains no specific provisions on the transfer of data within or between Community institutions. However, the general principles governing the processing of personal data continue to apply.

## Prior consultation of the EDPS (Article 40)

The controller must consult the EDPS when the DPIA indicates that, in the absence of safeguards, security measures and mitigating mechanisms, processing would result in a high risk to the rights and freedoms of natural persons.

Prior consultation is necessary only if the controller is of the opinion that the risks identified in the DPIA cannot be mitigated by means that are reasonable in terms of available technologies and cost of implementation. This prior consultation replaces the current prior checking for sensitive processing operations.

## Records of processing activities (Article 31)

Prior notification of the DPO is no longer mandatory. Instead, the controller (and the processor) must maintain records of all processing operations under their responsibility. These must be made available to the EDPS on request.

The new Regulation No 2018/1725 requires for institutions (safe for small-sized institutions and bodies) to keep a centralised register of activities, which should be publicly accessible

# Fines for non-compliance with data protection rules

## (Articles 66 and 29(10))

One key new element is the introduction of administrative fines for non-compliance with data protection rules.

The new Regulation No 2018/1725 authorises the EDPS to sanction another EU institution for failure to comply with one of its orders. For example an administrative fine can be imposed in case of failure by the controller to act on an order to:

* comply with the data subject’s request to exercise his or her rights;
* rectify or erase personal data, or restrict its processing; or
* suspend data flows to a recipient in a Member State, a non-EU country or an international organisation.

The level of the fine will be decided case by case and depend on what rule has been infringed. Fines can be up to EUR 25 000 per infringement and up to a total of EUR 250 000 per year. For major breaches, they can go up to EUR 50 000 per infringement and up to a total of EUR 500 000 per year.

Processors may also be subject to fines if they do not follow the controller’s instructions.

# Other provisions

## Data protection officer (Articles 43-45)

The main changes are that:

* a single DPO can be appointed for several Union institutions and bodies;
* the DPO will be appointed for a term of three to five years and the possibility of renewing the appointment is not limited (under Regulation (EC) No 45/2001, the DPO’s term of office cannot exceed 10 years);
* the DPO is expressly tasked with monitoring his/her institution’s compliance with the new Regulation, as well as with other data protection provisions and the institution’s personal data protection policies; this involves assigning responsibilities, awareness raising, training and audits; and
* the controller must inform the DPO about personal data breaches, and consult the DPO on DPIAs and prior consultation of the EDPS.

The DPO tasks can be outsourced.

## International data transfers (Article 46-51)

The new Regulation No 2018/1725 formalises the practice of recognising binding corporate rules as appropriate safeguards when Union institutions and bodies use an external processor to transfer personal data to countries or international organisations not covered by a Commission adequacy decision. International transfers can also be based on standard contractual clauses and a legally binding and enforceable instrument between public authorities and bodies.

The EDPS can authorise the insertion of other contractual clauses or provisions into administrative arrangements.

The new Regulation No 2018/1725 also provides that requests from judicial or administrative courts or authorities in non-EU countries for the transfer or disclosure of personal data can be enforced only if they are based on an international agreement (e.g. mutual assistance treaty).

## Specific provisions for archiving (Article 13)

The new Regulation No 2018/1725 introduces a provision on processing for archiving purposes; it underlines the need to put in place appropriate safeguards, such as pseudonymisation, to ensure data minimisation.



1. Disclaimer: This document provides a general overview of the key elements in the new Regulation (EU) No 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (the ‘EU Data Protection Regulation’). The text is amended by the CPVO DPO to reflect the necessary changes at the moment of making it available at the CPVO. [↑](#footnote-ref-1)
2. Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC of the European parliament and the Council of 24 October 1995 on the protection of individuals with regard to processing personal data and on the free movement of such data. [↑](#footnote-ref-2)
3. Regulation (EC) 45/2001 of the European Parliament and the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. [↑](#footnote-ref-3)
4. Accountability means that the controller is in charge of and responsible for ensuring compliance with all the principles relating to processing of personal data (see point 3.1 of this Guide) and being able to demonstrate that compliance. (EDPS: [Accountability on the ground: Provisional guidance on documenting processing operations for EU institutions, bodies and agencies](https://edps.europa.eu/data-protection/our-work/publications/guidelines/accountability-ground-provisional-guidance_en)). [↑](#footnote-ref-4)
5. Article 25 of the GDPR obliges controllers to "implement appropriate technical and organisational measures (…), which are designed to implement data protection principles, (…) and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects". The controller shall observe this obligation both "at the time of the determination of the means for processing", i.e. when the processing systems are designed, developed and tested, and "at the time of the processing itself," i.e. when the system is running in production mode. It shall further ensure that, "by default, only personal data which are necessary for each specific purpose of the processing are processed" (data protection by default). [↑](#footnote-ref-5)
6. Proposal for regulation of the EU Parliament and the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). [↑](#footnote-ref-6)