



## Data Protection

Data Protection Officer

Luxembourg, 8 June 2023

# Overview of data subject rights

Regulation (EU) 2018/1725<sup>1</sup> (the “**EUDPR**”) confers a panoply of rights upon individuals (“**data subjects**”)<sup>2</sup>.

- **Section 1** details the **common principles** regarding data subject rights requests with which controllers must comply.
- **Section 2** contains the list of **data subject rights**, together with the relevant principles, as well as the exceptions applicable in certain cases.

Court Decision No 42-2021<sup>3</sup> allows data subject rights to be restricted on a case-by-case basis, e.g., when the European Court of Auditors (the “**ECA**”) is “*carrying out audits on the basis of Article 287 TFEU*”<sup>4</sup>.

This document does not detail the controller’s other obligations to data subjects with regard to the processing of their personal data, e.g., the obligation to notify them of any personal data breach likely to result in a high risk to their rights and freedoms, etc.

## 1. Data subject rights – common principles

### (a) Deadline for reply

Principle	Exception
Upon receipt of a request from a data subject exercising their rights, the controller must inform the data subject of the action taken <b>without undue delay</b> and in any event <b>within one (1) month</b> of receipt of the request.	<p>This period may be <b>extended by two (2) further months</b> where necessary (depending on the complexity and number of requests).</p> <p>The data subject must be informed of the extension (if any) <b>within one (1) month</b> of receipt of the request, together with the reasons for the delay.</p>

<sup>1</sup> [Regulation \(EU\) 2018/1725](#) on the protection of natural persons 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) 45/2001 and Decision No 1247/2002/EC, which entered into force on 11 December 2018.

<sup>2</sup> A **data subject** is an identified or identifiable natural person, i.e. one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (see Article 3(1) [EUDPR](#)).

<sup>3</sup> [Decision No 42/2021](#) of 20 May 2021 adopting internal rules concerning restrictions of certain rights of data subjects in relation to the processing of personal data in the framework of activities carried out by the ECA.

<sup>4</sup> See Article 2(1)(a) of [Decision No 42/2021](#).

<p>If no action is taken, the data subject must be informed <b>within one (1) month</b> of receipt of the request:</p> <ul style="list-style-type: none"> <li>o of the reasons for no action being taken and</li> <li>o on the possibility of lodging a complaint with the European Data Protection Supervisor and seeking a judicial remedy.</li> </ul>	
--	--

Where the data subject submits the request electronically, the information must also be provided electronically, unless otherwise requested by the data subject.

## (b) Costs

Principle	Exception
The data subject must be able to exercise their rights <b>free of charge</b> .	<p><b>Where requests</b> from a data subject are manifestly <b>unfounded or excessive</b> (e.g. repetitive in nature), the controller <u>may refuse to act</u> on the request.</p> <p>The burden of demonstrating the manifestly unfounded or excessive nature of the request lies with the controller.</p>

## (c) Actions prior to fulfilling a request

Prior to responding to a data subject's request, the controller must confirm that the requester is who they say they are. If the controller has reasonable doubts concerning the identity of the person making the request, the data subject may be asked to provide additional information to confirm their identity.<sup>5</sup>

## 2. Data subject rights – list

### (a) Right to information (Articles 15 and 16)

Principle	Exception
The controller must provide data subjects with <b>clear and transparent information</b> (e.g. in a privacy statement), detailing the processing of their personal data, what their rights are, the legal basis, the purpose of the processing, to whom the data may be disclosed, and any other information required by Article 15 <a href="#">EUDPR</a> ' <i>Information to be provided where personal data are collected from the data subject</i> '.	<p>The obligation to provide information does not apply in the following cases:</p> <ul style="list-style-type: none"> <li>o the data subject already has the information. However, where the information is incomplete, the controller must supplement it accordingly (this applies to <b>personal data both collected directly and obtained indirectly</b>).</li> </ul>

<sup>5</sup> Article 14(6) of the EUDPR "Without prejudice to Article 12, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 17 to 23, the controller may request the provision of additional information necessary to confirm the identity of the data subject."

<p>In addition, where personal data have not been obtained directly from the data subjects, the controller must inform them of the source of the data, as required by Article 16 <a href="#">EUDPR</a> ‘<i>Information to be provided where personal data have not been obtained from the data subject</i>’.</p> <p>Where the provision of personal data is compulsory, the controller must also indicate the consequences of failure to provide the data requested.</p> <p>Information must be provided to the data subject:</p> <ul style="list-style-type: none"> <li>o in the event of <u>direct collection</u>, when personal data are collected, or</li> <li>o where personal data were <u>obtained indirectly</u>, within a “reasonable period” following the event, and in any case <b>no later than one (1) month</b>.</li> </ul>	<p>Where the personal data were obtained indirectly, the obligation to provide information does not apply in the following cases:</p> <ul style="list-style-type: none"> <li>o it is impossible to provide the information, or requires disproportionate effort;</li> <li>o obtaining or disclosing the information is expressly provided for under Union law;</li> <li>o where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union law.</li> </ul>
--	--

## (b) Right of access (Article 17)

Principle	Exception
<p>The data subject has the right to obtain confirmation of whether personal data concerning them are being processed. Where that is the case, the data subject must be granted access to the personal data, as well as to the information regarding the processing.<sup>6</sup></p> <p>The controller must provide a copy of the personal data being processed.<sup>7</sup></p>	<p>Where the controller holds a large quantity of data relating to the data subject, they may ask the data subject to specify the information or processing activities to which their request relates.</p> <p>Where granting access to the data would affect other rights (e.g., trade secrets, intellectual property rights), the controller may restrict or refuse to provide the data requested (following assessment).</p>

The purpose of this right is to allow the data subject to confirm the accuracy of their personal data and the lawfulness of the processing, as well as exercise their rights of correction, objection, etc., if necessary.

## (c) Right to rectification (Article 18)

Principle	Exception
<p>Data subjects can ask the controller to <b>rectify inaccuracies in their personal data</b>.</p>	<p>None.</p>

<sup>6</sup> In accordance with Article 17.1 EUDPR, the information regarding the processing includes the following: the purposes of processing, the categories of data processed, the recipients, or categories of recipients (in particular, details of disclosure to recipients in third countries), the envisaged retention period, or, if this is not possible, the criteria used to determine this period, the individual’s rights of rectification or erasure, or restriction of processing or to object to such processing, the individual’s right to lodge a complaint with the European Data Protection Supervisor (EDPS), information regarding the source of the data (if data not collected from the data subject), and the existence of automated decision-making, i.e. decisions taken solely on an automated basis and having legal or similar effects, including information about the logic involved and the significance and envisaged consequences of the processing for the data subject.

<sup>7</sup> This is not a copy of documents containing personal data, but of the actual personal data.

## (d) Right to erasure (“Right to be forgotten”) (Article 19)

Principle	Exception
Data subjects have the <b>right to have their data “erased”</b> in certain specific situations.	<p>The right to erasure does not apply when the processing is necessary:</p> <ul style="list-style-type: none"><li>○ for exercise of the right of freedom of expression and information;</li><li>○ to comply with a legal obligation or perform a task carried out in the public interest or in the exercise of official authority vested in the controller;</li><li>○ for reasons of public interest in the area of public health;</li><li>○ for archival, research or statistical purposes (insofar as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of the processing);</li><li>○ for the establishment, exercise or defence of legal claims.</li></ul>

This right applies in the following circumstances:

- when data are no longer necessary for the purpose for which they were collected or processed;
- where the data subject withdraws consent to the processing (and there is no other legal ground for the processing);
- the data subject objects to the processing and there are no overriding legitimate grounds for the processing;
- where the personal data have been unlawfully processed;
- where the personal data must be erased to comply with a legal obligation to which the controller is subject;
- where the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).<sup>8</sup>

## (e) Right to restriction of processing (Article 20)

Principle	Exception
This right is an <b>alternative to the right to erasure</b> . It allows the data subject to demand the suspension of the erasure whilst other challenges are being resolved.	None.

The right to restriction of processing applies when:

- the accuracy of the personal data is contested by the data subject, and for as long as the controller needs to verify the facts;
- the processing is unlawful and the data subject opposes the erasure and requests the restriction instead;
- the controller no longer needs the personal data, but they are required by the data subject for the establishment, exercise or defence of legal claims;

---

<sup>8</sup> Article 8.1 stipulates the legal base for the consent: “in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 13 years old. Where the child is below the age of 13 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child”.

- o the data subject has objected to the processing pending verification of whether the legitimate grounds of the controller override those of the data subject.

Where personal data are “restricted”, the controller **may only store the data**. They may not process the data further unless one of the following conditions applies:

- o the data subject consents;
- o the processing is necessary for the establishment, exercise or defence of legal claims;
- o the processing is necessary for protection of the rights of another natural or legal person;
- o the processing is necessary for reasons of important public interest of the Union or of a Member State.

The controller must notify the data subject before lifting a processing restriction.

## (f) Right to data portability (Article 22)

Principle	Exception
<p>The data subject has the right to:</p> <ul style="list-style-type: none"> <li>o receive personal data concerning them, which they themselves provided to a controller, in a structured, commonly used and machine-readable format, and</li> <li>o transmit those data to another controller without hindrance. The controller may be required to transmit the data directly to another controller, where technically feasible.</li> </ul>	<p><b>This right applies only when</b> the personal data requested are processed by automated means (excluding paper files) and the processing is based on <u>consent</u> or on a <u>contract</u> (including pre-contractual steps). Processing activities based on other legal bases are excluded, such as the processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Since the latter is the most common ground for the lawfulness of processing of personal data at the ECA, the scope of the right to data portability within the institution is rather limited.</p> <p>This right applies only to personal data that were <b>provided</b> by the data subject, including <b>observed</b> data provided by virtue of the data subject's use of the controller's service.</p> <p><b>This right shall not adversely affect the rights and freedoms of others.</b> Where the data set contains other data subjects' personal data (i.e., not those of the data subject seeking to exercise this right), their data must not be sent to the other controller.</p>

## (g) Right to object (Article 23)

Principle	Exception
<p>Data subjects have the rights to object to:</p> <ul style="list-style-type: none"> <li>o marketing (termed “opt-out”);</li> <li>o processing for the performance of a task in the public interest/exercise of official authority;</li> </ul>	<ul style="list-style-type: none"> <li>o With regard to opting out of marketing, there are no exceptions. This right is absolute. The data subject does not need to provide grounds for objection.</li> <li>o Upon receipt of an objection to processing for the performance of a task in the public interest/exercise of official authority, the controller must cease</li> </ul>

<ul style="list-style-type: none"> <li>o processing for scientific, historical-research or statistical purposes.</li> </ul> <p>Upon objection, the controller must cease processing the personal data, unless an exception applies.</p>	<p>processing the personal data, unless they can demonstrate compelling legitimate grounds for continuing such processing that override the interests, rights and freedoms of the data subject, or that is it necessary for the establishment, exercise or defence of legal claims.</p> <ul style="list-style-type: none"> <li>o Where personal data are processed for scientific, historical-research or statistical purposes, the data subject, <b>on grounds relating to their particular situation</b>, has the right to object to the processing of personal data concerning them, unless such processing is necessary for the performance of a task carried out in the public interest.</li> </ul>
---	--

## (h) Right not to be subject to a decision based solely on automated processing of personal data, including profiling (Article 24)

To prevent data subjects from being subject to decisions emanating solely from machines, the legislator has created a special legal framework applicable solely to automated decision-making, including profiling.

Principle	Exception
<p>The data subject has the right not to be subject to solely automated decisions, including profiling, which have a <b>legal or similarly significant effect</b> on them.</p>	<p>Exceptions are made when the decision is based on one of the following:</p> <ul style="list-style-type: none"> <li>o contractual necessity;</li> <li>o Union law;</li> <li>o the data subject's consent.</li> </ul> <p><u>Condition applicable in order for the exception to apply:</u> Data subjects have the right to obtain human intervention, meaning that the decision-making process requires meaningful supervision by someone with the authority and competence to change the decision. The minor involvement of a natural person who has no power to overwrite the decision is not sufficient.</p> <p>Where <b>special categories of personal data</b> are involved, automated decision-making cannot take place unless the following <u>cumulative conditions</u> are met:</p> <ol style="list-style-type: none"> <li>1) one of the above exceptions applies (contractual necessity, Union law or consent);</li> <li>2) subparagraph (a) (the data subject has explicitly consented) or (g) (the processing is necessary for reasons of substantial public interest, on the basis of Union law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject) of Article 10(2) applies.</li> <li>3) Suitable measures to safeguard the data subject's rights, freedoms and legitimate interests are in place.</li> </ol>