

Issue	The Directive	The GDPR	Impact
<p><b>Transparent communication</b></p> <p>In order to ensure that personal data are processed fairly, EU data protection law obliges controllers to communicate transparently with data subjects regarding the processing of their personal data.</p>	<p><b>Rec.38, 40; Art.10</b></p> <p>The Directive obliges controllers to provide certain minimum information to data subjects, regarding the collection and further processing of their personal data.</p>	<p><b>Rec.39, 58, 60; Art.5(1)(a), 12-14</b></p> <p>In order to ensure that personal data are processed fairly and lawfully, controllers must provide certain minimum information to data subjects, regarding the collection and further processing of their personal data. <b>Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.</b> Any information provided to children should be in such a clear and plain language that the child can easily understand.</p>	<p><b>⊖</b></p> <p>Although the language in the GDPR differs from that in the Directive, national DPAs in Member States have consistently interpreted the Directive in a similar vein, requiring controllers to provide information that is transparent, concise, etc. Consequently, the practical impact of this change is fairly limited. The information given to the data subject should not consist of privacy policies that are excessively lengthy or difficult to understand.</p>
<p><b>Rights of data subjects</b></p> <p>Controllers are obliged to give effect to the rights of data subjects under EU data protection law.</p>	<p><b>N/A</b></p> <p>The Directive does not directly oblige controllers to give effect to the rights of data subjects (although this is implied).</p>	<p><b>⊖</b></p> <p><b>Rec.59; Art.12(2)</b></p> <p>Controllers have a <b>legal obligation to give effect to the rights of data subjects.</b></p>	<p><b>⊖</b></p> <p>In effect, controllers are required to give effect to the rights of data subjects under the Directive. The GDPR merely formalises the de facto position under the Directive.</p>
<p><b>Identifying data</b></p>		<p><b>⊖</b></p> <p><b>Rec.57, 64; Art.12(2),</b></p>	<p><b>⊕</b></p> <p>The GDPR</p>

<p><b>subjects</b></p> <p>Third parties might attempt to exercise a data subject's rights without proper authorisation to do so. Controllers are therefore permitted to ask data subjects to provide proof of their identity before giving effect to their rights.</p>	<p><b>N/A</b></p> <p>The Directive does not directly address the need to confirm the identity of data subjects (although the national laws of many Member States do so).</p>	<p><b>(6)</b></p> <p>The controller must not refuse to give effect to the rights of a data subject unless the controller cannot identify the data subject. <b>The controller must use all reasonable efforts to verify the identity of data subjects. Where the controller has reasonable doubts as to the identity of the data subject, the controller may request the provision of additional information necessary to confirm the identity of the data subject, but is not required to do so</b> (see the row immediately below).</p>	<p>explicitly enables controllers to require data subjects to provide proof of identity before giving effect to their rights. This helps to limit the risk that third parties gain unlawful access to personal data. However, the GDPR does not oblige controllers to seek out information to identify data subjects (see the row immediately below).</p>
<p><b>Exemption where the controller cannot identify the data subject</b></p> <p>If the controller cannot identify the data subject, the controller is exempt from the application of certain rights of that data subject.</p>	<p><b>N/A</b></p> <p>The Directive does not directly address the circumstances in which a controller cannot identify data subjects.</p>	<p><b>Rec.57; Art.11, 12(2)</b></p> <p>To the extent that the controller can demonstrate that it is not in a position to identify the data subject, the controller <b>is exempt from the application of the rights of data subjects</b> in <b>Art.15-22</b>. The controller is also <b>not obliged to obtain further personal data</b> in order to link data in its possession to a data subject.</p>	<p>Under the GDPR the controller is exempt from its obligation to comply with certain rights of data subjects if it cannot identify which data in its possession relate to the relevant data subject.</p>



<p><b>Time limits for complying with the rights of data subjects</b></p> <p>Controllers are obliged to give effect to the rights of data subjects within specified time periods, in order to avoid the frustration of those rights through excessive delays.</p>	<p><b>N/A</b></p> <p>The Directive does not specify time limits for compliance with the rights of data subjects. However, the time limits may be specified under national law.</p>	<p><b>Rec.59; Art.12(3)-(4)</b></p> <p>A controller must, <b>within one month</b> of receiving a request made under those rights, provide any requested information in relation to <b>any of the rights of data subjects</b>. If the controller fails to meet this deadline, the data subject may complain to the relevant DPA and may seek a judicial remedy. Where a controller receives large numbers of requests, or especially complex requests, <b>the time limit may be extended by a maximum of two further months</b>.</p>	<p>The introduction of specified time limits under the GDPR results in more onerous compliance obligations for controllers.</p>
<p><b>Right to basic information</b></p> <p>A core principle of EU data protection law is that data subjects should be entitled to a minimum set of information concerning the purposes for which their personal data will be processed.</p>	<p><b>Rec.38; Art.10, 11</b></p> <p>Data subjects have the right to be provided with information on the identity of the controller, the controller's reasons for processing their personal data and other relevant information necessary to ensure the fair processing of personal data.</p>	<p><b>Rec.58, 60; Art.13-14</b></p> <p>Data subjects have the right to be provided with information on the identity of the controller, the reasons for processing their personal data and other relevant information necessary to ensure the fair <b>and transparent</b> processing of personal data.</p>	<p>The GDPR largely preserves the position as it stands under the Directive—the requirement to ensure transparency is implied in the Directive. Organisations remain obliged to provide basic information to individuals.</p>
<p><b>Right of access</b></p> <p>In order to allow data subjects to</p>	<p><b>Rec.27, 41-44; Art.12(a)</b></p> <p>Data subjects have</p>	<p><b>Rec.63; Art.15</b></p> <p>Data subjects have the right to obtain the</p>	<p>The GDPR expands the mandatory categories of</p>

enforce their data protection rights, EU data protection law obliges controllers to provide data subjects with access to their personal data.

the right to obtain:

- confirmation of whether the controller is processing their personal data;
- information about the purposes of the processing;
- information about the categories of data being processed;
- information about the categories of recipients with whom the data may be shared;
- a copy of those data (in an intelligible format) and information as to the source of those data; and
- an explanation of the logic involved in any automated processing that has a significant effect on data subjects.

following:

- confirmation of whether, and where, the controller is processing their personal data;
- information about the purposes of the processing;
- information about the categories of data being processed;
- information about the categories of recipients with whom the data may be shared;
- information about **the period for which the data will be stored** (or the criteria used to determine that period);
- information about **the existence of the rights to erasure, to rectification, to restriction of processing and to object to processing;**
- information about **the existence of the right to complain to the DPA;**
- **where the data were not**

information which must be supplied in connection with a data subject access request. Such requests are therefore likely to place an even greater administrative burden on organisations than that which is currently experienced.



The Directive and the GDPR both note that the exercise of the right of access by data subjects should not adversely affect an organisation's intellectual property (i.e., giving effect to the right of access should not require the disclosure of trade secrets, etc.). However, cases in which trade secrets and other intellectual property rights fall within the scope of the right of access are likely to be rare.

- collected from the data subject,**  
 information as to the source of the data; and
- information about **the existence of,**  
 and an explanation of the logic involved in, any automated processing that has a significant effect on data subjects.

Additionally, data subjects may request a copy of the personal data being processed.



**Fees in respect of access requests**

In order to dissuade data subjects from making vexatious requests, data controllers are permitted to charge a small fee for each such request.

**Art.12(a)**

The right of access must be provided without excessive delay or expense. It is up to Member States to determine any maximum fee, but generally the maximum is very low (e.g., the UK has a maximum of £10 per request).

**Rec. 59; Art.12(5), 15(3), (4)**

The controller must give effect to the rights of access, rectification, erasure and the right to object, **free of charge**. The controller may charge a reasonable fee for "repetitive requests", "manifestly unfounded or excessive requests" or "further copies".

The Directive permits controllers to charge a small fee for certain functions (e.g., responding to the right of access). This acts as a buffer against spurious requests. The GDPR does not permit such charges in most cases. There is, therefore, an elevated risk that individuals will attempt to exercise these rights merely because they can, or as a cheap but effective means of protest against an organisation.

## Right of rectification

Data subjects are entitled to require a controller to rectify any errors in their personal data.

**Art.6(1)(d), 12(b)**

Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to have personal data rectified where the controller fails to comply with the Directive (especially where the data are inaccurate or incomplete).



**Rec.39, 59, 65, 73; Art.5(1)(d), 16**

Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to rectification of inaccurate personal data.



The position under the GDPR is largely unchanged, and organisations are likely to face the same requirements under the GDPR as under the Directive, in relation to the right of rectification.

## Right to erasure (the "right to be forgotten")

Data subjects are entitled to require a controller to delete their personal data if the continued processing of those data is not justified.

**Art.12(b)**

Data subjects have the right to have personal data erased or "blocked" where the controller fails to comply with the Directive (especially where the data are inaccurate or incomplete).



**Rec.65-66, 68; Art.17**

Data subjects have the right to erasure of personal data (the "right to be forgotten") if:

- **the data are no longer needed for their original purpose** (and no new lawful purpose exists);
- **the lawful basis for the processing is the data subject's consent**, the data subject withdraws that consent, and no other lawful ground exists;
- the data subject exercises the right to object, and the



The GDPR creates a broader right to erasure than the right available to data subjects under the Directive. Consequently, organisations face a broader spectrum of erasure requests with which they must comply.

- controller has no overriding grounds for continuing the processing;
- the data have been processed unlawfully; or
- erasure is **necessary for compliance with EU law or the national law of the relevant Member State.**



**The right to restrict processing**

In some circumstances, data subjects may not be entitled to require the controller to erase their personal data, but may be entitled to limit the purposes for which the controller can process those data (e.g., the exercise or defence of legal claims; protecting the rights of another person or entity; purposes that serve a substantial public interest; or such other purposes as the data subject may consent to).

N/A

The Directive does not directly address the right to restrict processing. However, the Directive does provide for the right to request the blocking of data under **Art.12(b)-(c)**. This means that the controller must refrain from using the data during the period for which that right applies, even though the data have not yet been deleted.

**Rec.67; Art.18**

Data subjects have the **right to restrict the processing of personal data** (meaning that the data may only be held by the controller, and may only be used for limited purposes) if:

- the **accuracy of the data is contested** (and only for as long as it takes to verify that accuracy);
- the **processing is unlawful and the data subject requests restriction** (as opposed to exercising the right to erasure);
- the controller **no longer needs the data for their original**

Under the GDPR, in addition to the right to erasure (or "right to be forgotten"— see above) organisations face a much broader range of circumstances in which data subjects can require that the processing of their personal data is restricted.

**purpose**, but the data are still required by the controller to establish, exercise or defend legal rights; or

- if **verification of overriding grounds** is pending, in the context of an erasure request.



**Notifying third parties regarding rectification, erasure or restriction**

It is only possible to give full effect to the rights of data subjects if all parties who are processing the relevant data are aware that the data subject has exercised those rights. Therefore, controllers must notify any third parties with whom they have shared the relevant data that the data subject has exercised those rights.

**Art.12(c)**

Where a controller has disclosed personal data to any third parties, and the data subject has subsequently exercised any of the rights of rectification, erasure or blocking, the controller must notify those third parties of the data subject's exercising of those rights. The controller is exempt from this obligation if it is impossible or would require disproportionate effort.

**Rec.62; Art.17(2), 19**

Where a controller has disclosed personal data to any third parties, and the data subject has subsequently exercised any of the rights of rectification, erasure or blocking, the controller must notify those third parties of the data subject's exercising of those rights. The controller is exempt from this obligation if it is impossible or would require disproportionate effort. **The data subject is also entitled to request information about the identities of those third parties. Where the controller has made the data public, and the data subject exercises these rights, the controller must take reasonable steps (taking costs into account) to inform third parties that the**

In addition to implementing systems and procedures for giving effect to the new rights that the GDPR grants to data subjects, organisations are also required to implement systems and procedures for notifying affected third parties about the exercise of those rights. For organisations that disclose personal data to a large number of third parties, this may be particularly burdensome.



**Right of data portability**

Data subjects have the right to transfer their personal data between controllers (e.g., to move account details from one online platform to another).

The WP29 has issued [Guidelines on Data Portability \(WP 242\)](#) (the "Data Portability Guidelines") which provide further clarity on the concept of data portability.

N/A

The Directive does not directly address the right of data portability.

**data subject has exercised those rights.**



**Rec.68, 73; Art.20; WP29 Data Portability Guidelines**

Data subjects have a right to:

- receive a copy of their personal data in a structured, commonly used, machine-readable format that supports re-use;
- transfer their personal data from one controller to another;
- store their personal data for further personal use on a private device; and
- have their personal data transmitted directly between controllers without hindrance.

Inferred data and derived data (e.g., a credit score or the outcome of a health assessment) do not fall within the right to data portability, because such data are not "provided by the data subject". In addition, the controller is not



For some organisations, this new right to transfer personal data between controllers creates a significant additional burden, requiring substantial investment in new systems and processes. The WP29 considers that controllers should:

- create simple mechanisms for giving effect to this right (e.g., direct download tools);
- ensure the interoperability of the data format provided in the exercise of a data portability request; and
- allow data subjects to directly transmit the data to another controller.

obliged to retain personal data for longer than is otherwise necessary, simply to service a potential data portability request.



For some organisations, the right to transfer personal data between controllers creates a significant opportunity to attract customers from competitors (e.g., online businesses and social media networks can attract users who were formerly unwilling to move from a competitor, because of the difficulties associated with setting up a new account—under the GDPR, the competitor must allow the account information to simply be transferred).



**Right to object to processing**

As set out [in Chapter 7](#), a controller must have a lawful basis for processing personal data. However, where that lawful basis is either "public interest" or "legitimate

**Rec.30, 45; Art.14(a)**

Data subjects have the right to object, on any compelling legitimate grounds, to the processing of personal data, where the basis for that processing is either:

- public interest; or
- legitimate interests of the

**Rec.50, 59, 69-70, 73; Art.21**

Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data, where the basis for that processing is either:

- public interest; or
- legitimate

The Directive permits an organisation to continue processing the relevant data unless the data subject can show that the objection is justified. The GDPR reverses the burden, and requires the organisation to demonstrate that

<p>interests", those lawful bases are not absolute, and data subjects may have a right to object to such processing.</p>	<p>controller.</p> <p>Where the data subject's objection is justified, the controller must cease the relevant processing activity in relation to those data.</p>	<p>interests of the controller.</p> <p>The controller <b>must cease such processing unless</b> the controller:</p> <ul style="list-style-type: none"> <li>• demonstrates <b>compelling legitimate grounds for the processing</b> which override the interests, rights and freedoms of the data subject; or</li> <li>• <b>requires the data in order to establish, exercise or defend legal rights.</b></li> </ul>	<p>it either has compelling grounds for continuing the processing, or that the processing is necessary in connection with its legal rights. If it cannot demonstrate that the relevant processing activity falls within one of these two grounds, it must cease that processing activity. This will be especially problematic for organisations that currently rely on their own legitimate interests as a lawful basis for processing personal data.</p>
--	--	---	---



**Right to object to processing for the purposes of direct marketing**

Data subjects have the right to object to the processing of their personal data for the purposes of direct marketing.

**Rec.30; Art.14(b)**

Data subjects have the right to object to the processing of personal data for the purpose of direct marketing.

**Rec.70; Art.21(2)-(3)**

Data subjects have the right to object to the processing of personal data for the purpose of direct marketing, including profiling.



The GDPR preserves the position as it stands under the Directive. It should be noted that data subjects also have rights in respect of direct marketing under the ePrivacy Directive ([see Chapter 18](#)).



**Right to object to processing for**

**Rec.156; Art.21(6),**



In effect, the GDPR is giving

**scientific, historical or statistical purposes**

Personal data may be processed for scientific, historical or statistical purposes in the public interest, but individuals have a right to object to such processing.

The Directive does not provide a specific right to object to processing of this type, but note the general right to object to processing set out above.

**83(1)**

Where personal data are processed for **scientific and historical research purposes or statistical purposes, the data subject has the right to object**, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

individuals a more specific right to object than the rights available under the Directive. In practice, this is likely to make little difference for most organisations.

**Obligation to inform data subjects of the right to object**

Controllers are obliged to inform data subjects of their rights to object to processing.

N/A

The Directive does not provide a specific obligation to inform data subjects of these rights.



**Art.13(2)(b), 14(2)(c), 15(1)(e), 21(4)**

**The right to object to processing of personal data noted above must be communicated to the data subject no later than the time of the first communication with the data subject.**

This information should be provided clearly and separately from any other information provided to the data subject.



Controllers are obliged to provide additional information to data subjects. For many organisations, this will require revisions to standard data protection policies and privacy notices.

**Right to not be evaluated on the basis of automated processing**

Data subjects have the right not to be evaluated in any material

**Rec.11, 15, 27, 41; Art.15**

Data subjects have the right not to be subjected to decisions based solely on automated processing of data for the purpose of personal

**Rec.71, 75; Art.22**

Data subjects have the right not to be subject to a decision based solely on automated processing which significantly affect them (including profiling). Such processing is

sense (e.g., in connection with offers of employment; supermarket discounts; insurance premiums; or howsoever) solely on the basis of automated processing of their personal data.

evaluation. Such processing is permitted where:

- it is performed in the course of entering into a contract with the data subject, provided that appropriate safeguards are in place; or
- it is authorised by law.

permitted where:

- it is necessary for entering into or performing a contract with the data subject provided that appropriate safeguards are in place;
- it is authorised by law; or
- **the data subject has explicitly consented and appropriate safeguards are in place.**