### Issue

### The Directive

### The GDPR

## **Impact**



### **Transparent** communication

## Rec.38, 40; Art.10

# Rec.39, 58, 60;

left



that personal data certain minimum are processed fairly, EU data protection law to communicate transparently with data subjects regarding the processing of their personal data.

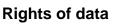
The Directive obliges In order to ensure controllers to provide information to data subjects, regarding the collection and obliges controllers further processing of their personal data.

Art.5(1)(a), 12-14

In order to ensure that personal data are processed fairly and lawfully, controllers must provide certain minimum information to interpreted the data subjects, regarding the collection similar vein, and further processing of their personal data. Such information must be provided in a information that is concise, transparent, intelligible and easily accessible form, using clear and plain language. Any information provided to fairly limited. The children should be in such a clear and plain language that the child can easily understand.

Although the language in the GDPR differs from that in the Directive, national DPAs in Member States have consistently Directive in a requiring controllers to provide transparent, concise, etc. Consequently, the practical impact of this change is information given to the data subject should not consist of privacy policies that are excessively lengthy or difficult to understand.





## subjects

Controllers are obliged to give of data subjects under EU data protection law.

## N/A

The Directive does not directly oblige controllers to give effect to the rights effect to the rights of data subjects (although this is implied).

## Rec.59; Art.12(2)

Controllers have a legal obligation to give effect to the rights of data subjects.



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.



Rec.57, 64; Art.12(2),

The GDPR

a

**Identifying data** 

## subjects

Third parties might attempt to exercise a data subject's rights without proper authorisation to are therefore permitted to ask data subjects to provide proof of their identity before giving effect to their rights.

### N/A

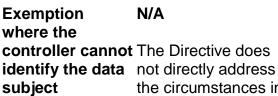
The Directive does not directly address the need to confirm the identity of data subjects (although the controller cannot national laws of many do so. Controllers Member States do so).

## **(6)**

The controller must not require data refuse to give effect to the rights of a data subject unless the identify the data subject. The controller helps to limit the must use all reasonable efforts to verify the identity of data subjects. Where the controller has reasonable doubts as GDPR does not to the identity of the data subject, the controller may request the provision identify data of additional information necessary to confirm below). the identity of the data subject, but is not required to do so (see the row immediately below).

explicitly enables controllers to subjects to provide proof of identity before giving effect to their rights. This risk that third parties gain unlawful access to personal data. However, the oblige controllers to seek out information to subjects (see the row immediately





application of

certain rights of

that data subject.

the circumstances in which a controller cannot identify data If the controller cannot identify the subjects. data subject, the controller is exempt from the

Rec.57; Art.11, 12(2)

To the extent that the controller can demonstrate that it is not in a position to identify the data subject, the controller is exempt from the application of the rights of data subjects in Art.15-22. The controller is also not obliged to obtain further personal data in order to link data in its possession to a data subject.



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.





## Time limits for complying with the rights of data The Directive does subjects

Controllers are obliged to give of data subjects within specified time periods, in order to avoid the frustration of those rights through excessive delays.

## N/A

not specify time limits for compliance with the rights of data subjects. However, specified under national law.

## Rec.59; Art.12(3)-(4)

A controller must. within one month of receiving a request made under those rights, provide any effect to the rights the time limits may be requested information in relation to any of the rights of data subjects. 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, the time limit may be extended by a maximum of two further months.

The introduction of specified time limits under the GDPR results in more onerous compliance obligations for controllers.





## Right to basic information

A core principle of the right to be EU data protection law is that data subjects identity of the should be entitled controller, the of information concerning the purposes for which their personal data will to ensure the fair be processed.

## Rec.38; Art.10, 11

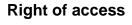
Data subjects have provided with information on the to a minimum set controller's reasons for processing their personal data and other relevant information necessary transparent processing of personal data.

## Rec.58, 60; Art.13-14

Data subjects have the position as it 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 **and** processing of personal data.

The GDPR largely preserves the stands under the Directive—the requirement to ensure transparency is implied in the Directive. **Organisations** remain obliged to provide basic information to individuals.





In order to allow data subjects to

## Rec.27, 41-44; Art.12(a)

Data subjects have

Data subjects have the mandatory right to obtain the

Rec.63; Art.15

The GDPR expands the categories of enforce their data the right to obtain: protection rights,

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

- 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 rights to erasure. to rectification, to cases in which restriction of to object to processing; information
- about the existence of the to be rare. 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 existence of the the disclosure of trade secrets. etc.). However, trade secrets and processing and other intellectual property rights fall within the scope of the right of access are likely

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.



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

The controller must give effect to the rights functions (e.g., delay or expense. It is of access, rectification, erasure and the right to right of access). object, free of charge. The controller may charge a reasonable fee for "repetitive requests", "manifestly unfounded or excessive charges in most requests" or "further copies".

The Directive permits controllers to charge a small fee for certain responding to the This acts as a buffer against spurious requests. The GDPR does not permit such 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.

## 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 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).





## Right of rectification

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

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

Controllers must Data subjects are ensure that inaccurate Controllers must or incomplete data are erased or rectified. Data subjects have the 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

ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to have personal 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 Art.12(b) (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.

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

- 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 than the right available to data subjects under the Directive. Consequently, the data are no 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. not be entitled to require the controller to erase of data under their personal data, but may be means that 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, personal data data subjects may the Directive does request the blocking Art.12(b)-(c). This entitled to limit 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 (meaning that the data organisations face provide for the right to may only be held by the a much broader controller, and may only be used for limited circumstances in purposes) if:

- the accuracy of require that the the data is contested (and personal data is 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) range of which data subjects can processing of their

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 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 require 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 data subjects if all rights of rectification, erasure or blocking. the controller must notify those third parties of the data subject's exercising of controller is exempt those rights. The controller is exempt is impossible or would effort. The data disproportionate effort.

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

Where a controller has

disclosed personal data procedures for to any third parties, and giving effect to the the data subject has subsequently exercised GDPR grants to any of the rights of rectification, erasure or organisations are blocking, the controller must notify those third parties of the data subject's exercising of those rights. The from this obligation if it is impossible or would from this obligation if it require disproportionate organisations that subject is also entitled to request information about the parties, this may 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 new rights that the data subjects, also required to implement systems and procedures for notifying affected third parties about the exercise of those rights. For disclose personal data to a large number of third be particularly burdensome.

## data subject has exercised those rights.





## 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.

## Rec.68, 73; Art.20; WP29 Data Portability organisations, this Guidelines

Data subjects have a right to:

- their personal data in a structured. commonly used, systems and machinethat supports re- that controllers 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 new right to transfer personal data between controllers creates a significant receive a copy of additional burden, requiring substantial investment in new processes. The readable format WP29 considers should:
  - create simple mechanism s for giving effect to this right (e.g., direct download tools):
  - ensure the interoperab ility 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 For some portability request.



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

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

- public interest; or
- legitimate interests of the

### Rec.30, 45; Art.14(a) Rec.50, 59, 69-70, 73; Art.21

Data subjects have the continue right to object, on legitimate grounds, to grounds relating to their relevant data 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 processing the unless the data subject can show that the objection is justified. The **GDPR** reverses the burden, and requires the organisation to demonstrate that

interests", those lawful bases are not absolute, and Where the data have a right to object to such processing.

controller.

data subjects may subject's objection is justified, the controller cease such must cease the relevant processing activity in relation to those data.

interests of the controller.

The controller must processing unless the that the controller:

- demonstrates compelling **legitimate** processing which override the interests, rights and data subject; or
- requires the data in order to activity. This will establish. exercise or defend legal rights.

it either has compelling grounds for continuing the processing, or processing is necessary in connection with its legal rights. If it cannot grounds for the demonstrate that the relevant processing activity falls within one of these two freedoms of the grounds, it must cease that processing

> be especially problematic for organisations that currently rely on their own legitimate interests as a lawful basis for processing personal data.



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 position as it right to object to the processing of personal data for the purpose of direct marketing. including profiling.

The GDPR preserves the 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).



Rec.156; Art.21(6),

In effect, the GDPR is giving

Right to object N/A to processing for

## 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 historical research to processing set out above.

## 83(1)

Where personal data are processed for scientific and 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 The right to object to obligation to inform rights.

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

processing of data subjects of these personal data noted above must be communicated to the will require data subject no later than the time of the first communication with the data subject. and privacy

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



## Right to not be evaluated on the Art.15 basis of automated

Data subjects to be evaluated in of data for the any material

processing

# Rec.11, 15, 27, 41;

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

## Rec.71, 75; Art.22

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



Controllers are obliged to provide additional information to data subjects. For organisations, this revisions to standard data protection policies notices.

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.