information commissioner
Barrantagh Fysseree

A closer look at

Rights & remedies

Important

This document is part of a series, produced purely for guidance, and does not constitute legal advice or legal analysis.

All organisations that process data need to be aware that the General Data Protection Regulation may apply directly to them.

The responsibility to become familiar with the GDPR and comply with its provisions from 25th May 2018 onwards lies with the organisation.

Legal advice, if required, should be sought from a Manx advocate.

INDEX

AN OVERVIEW OF THE RIGHTS & REMEDIES

The GDPR establishes a number of rights and remedies in relation to the processing of personal data.

Rights

The rights explained in this document can only be exercised against controllers. Failure to comply with rights is subject to the corrective powers of the supervisory authority and attracts the higher tier of administrative fine. (Article 58 & 83)

Controllers need to understand these rights in order to respond in a timely and appropriate manner when rights are exercised and to ensure that details of the rights are included in information provided to data subjects under the transparency requirements (the right to be informed under Articles 13 & 14).

Article 12 sets out general rules in respect of duties and procedural aspects of the rights, together with exceptions to those general rules.

Articles 15 - 22 prescribe the rights of individuals, which are:

- Right of access
- Right to rectification
- Right to erasure ('right to be forgotten')
- Right to restriction of processing
- Right to data portability
- Right to object to processing

Articles 23 and 85-90 set out restrictions on some of the rights of individuals which are to be provided for in Member State law. **Recital 73** provides further information regarding the restrictions.

AN OVERVIEW OF THE RIGHTS & REMEDIES

Remedies

Individuals have remedies in respect of the processing of their personal data.

These can be exercised against **controllers and processors** (to the relevant extent).

The remedies set out in **Articles 77, 79, 80 and 82** are:

- Right to lodge a complaint with a supervisory authority
- Right to an effective judicial remedy against a controller or processor
- Right to appoint a body to represent them in respect of the exercise of the rights under Articles 77 and 79 (i.e. the two points above)
- Right to compensation from controllers and processors

RIGHTS

Using this document

It is suggested that controllers firstly read the section on the general rules, exceptions and restrictions, which includes their duties and procedural aspects of complying with rights, and then consider the detail and application of a particular right.

This document also highlights, as applicable, the complementary links between rights and compliance with the principles and the inter-relationship of some of the rights.

RIGHTS - GENERAL RULES AND EXCEPTIONS

General rules applying to <u>all</u> the rights (set out in Article 12 and recital 59)

- Controllers must "facilitate**"** individuals to exercise their various rights
- Controllers must respond to individuals' requests to exercise rights and, where requests are made electronically, the information should, as far as possible, be provided electronically unless otherwise requested by the individual
- All communications and actions taken by the controller are generally free of charge*****
- Communications must be in a clear, concise, transparent, intelligible, and easily accessible form, using plain and clear language, particularly when addressed to children or other vulnerable groups
- Controllers may seek additional information to identify the individual exercising their rights if it has "reasonable doubts" concerning their identity (not applicable to Article 22)
- Compliance must be "without undue delay" and in most circumstances within ONE month******

Exceptions from the general rules applying to <u>all</u> the rights

<u>Fees</u> *****

- If requests are manifestly unfounded or excessive, particularly due to repetition of the same request, controllers may charge a reasonable fee (based on administrative costs) or refuse to act.
    - the controller must be able to demonstrate why it believed the request to be manifestly unfounded or excessive.

<u>Compliance period</u> ******

- The compliance period is without undue delay and in any event within one month of receipt.
- This can be extended by a maximum of TWO months, if necessary, where the requests are particularly complex or due to the volume of requests received.
    - the reason for the delay must be explained to the individual within ONE month of receipt of the request.

<u>Non-compliance with requests to exercise rights in relation to data</u>

- If action is not being taken by the controller on receipt of a request to exercise any right, it must inform the individual "without delay" (and within ONE month of receipt of the request) about:
    - the reasons for not taking action; and
    - their remedies, in particular the right to lodge a complaint with a supervisory authority (under Article 77) and to seek a judicial remedy (under Article 79)

RIGHTS - GENERAL RESTRICTIONS

A controller may refuse to comply with a request by an individual to exercise their rights where a **restriction** applies. Restrictions must be set out in Member State law and *"should be in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms"*.

Restrictions must respect *"the essence of the fundamental rights and freedoms and [be] a necessary and proportionate measure in a democratic society to safeguard"* the interests specified in **Article 23:**

(a) national security;

(b) defence;

(c) public security;

d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;

(f) the protection of judicial independence and judicial proceedings;

(g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);

(i) the protection of the data subject or the rights and freedoms of others, (inc. social protection, public health and humanitarian purposes (Rec 73)

(j) the enforcement of civil law claims.

Articles 85-90 variously require, or permit, Member States to create their own law in specific areas of processing which may include other restrictions on rights.

The interests requiring safeguarding set out in Article 23 and the specific areas of processing referred to in Articles 85-90 are consistent with the current 'exemptions'.

RIGHT OF ACCESS

"Right of access by the data subject"

What the law says

Article 15

1. *The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:*

   (a) the purposes of the processing;

   (b) the categories of personal data concerned;

   (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

   (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

   (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

   (f) the right to lodge a complaint with a supervisory authority;

   (g) where the personal data are not collected from the data subject, any available information as to their source;

   (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. *Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.*

3. *The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.*

4. *The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.*

"Right of access by the data subject"

What the law says

Recital 63

A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided.

Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are *processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing.*

Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data.

That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject.

Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.

"Right of access by the data subject"

The right of access is possibly the most important of the rights and is broadly equivalent to the right that already exists.

Controllers should, however, be aware that the definitions of 'personal data' and 'filing system' have been expanded and so, accordingly, has the scope of the right of access.

Controllers are expressly required to bring the right of access to the attention of data subjects under their transparency obligations and must be able to facilitate the exercise of the right.

The four elements to the right are summarised as follows:

1. **Confirmation** as to whether or not personal data concerning him or her are being processed:

I*f it is being processed*:

2. A**ccess** to the personal data:

3. I**nformation** about (described as the "right to know" in Rec 63) :
    a) the purposes of the processing;
    b) the categories of personal data concerned;
    c) the recipients or categories of recipient;
    d) the retention period;
    e) the rights of rectification, erasure , restriction and objection;
    f) the right to lodge a complaint with a supervisory authority;
    g) any available information as to their source, if they were not collected from the data subject;
    h) the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and possible consequences of that processing for the data subject.

and *if it is being transferred outside the EU*:

4. **Information** about the safeguards in place.

"Right of access by the data subject"

- in practice

Actions:	• **must respond** to the data subject to advise them whether personal data is, or is not, being processed. If personal data is being processed, the controller: • **shall** provide **a** copy of the personal data undergoing processing. • **should** provide the information in a commonly used electronic format if the request was made electronically, unless the data subject specifies otherwise.
Timing:	Response must be without undue delay and at the latest within one calendar month (See 'general rules and exceptions').
Identification:	Controllers may take 'reasonable measures' to identify the person making the request. (See 'general rules and exceptions')
Fees:	Controllers cannot charge a fee for complying with a request. (See 'general rules and exceptions')
Refusals:	The right to obtain a copy of the personal data is not absolute and the controller may refuse to comply with all or part of the request. However, the controller must be able to justify its decision to refuse to comply. Requests may be refused in cases where: • the request is manifestly unfounded or excessive, in particular if it is repetitive (Art 12(5)); • the rights and freedoms of others are adversely affected by the provision of the information to the data subject (Art 15(4)) • a restriction on the right can be justified in the particular circumstances (Art 23). This, as under the existing law, does not mean that the data subject is necessarily refused access to all the information about them and the request for access should be complied with as fully as possible.
Other points:	• Controllers should make it easy for data subjects to exercise their right (Art 12(2) & Rec 63) • Direct remote access to personal data via a secure system is encouraged where possible (Rec 63) • Transparency information must include reference to this right

RIGHT TO RECTIFICATION

"Right to rectification"

What the law says

Article 16

> *"The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of a supplementary statement."*

Article 19

> *"The controller shall communicate any rectification ... carried out in accordance with Article 16 ... to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it."*

Accurate personal data is important, particularly where decisions are made about individuals based on that information. This right provides for an individual to have inaccurate personal data rectified and the completion of incomplete personal data and is broadly equivalent to the right that already exists.

This right complements the 'accuracy' principle (Article 5(1)(d)) which imposes a duty on controllers to:

- keep personal data accurate and, where necessary, up to date; and
- take every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

"Right to rectification"

- in practice

Controllers must facilitate the exercise of an individuals right to:

- Rectification of inaccurate personal data; and/or
- The completion of incomplete personal data

Correction, or completion, of existing personal data is not always appropriate or possible but, in such circumstances, the right does provide for inclusion of a "**supplementary statement"** in the record.

Actions:	• **respond** to the individual to advise them on the action, or inaction, taken on their request; • **communicate** details of the recipients of the inaccurate data to the individual if they so request; • **communicate** any rectification to recipients of the inaccurate data, unless it proves impossible or involves disproportionate effort.
Timing:	Response must be without undue delay and at the latest within one calendar month (See 'general rules and exceptions').
Identification:	Controllers may take 'reasonable measures' to identify the person making the request. (See 'general rules and exceptions')
Fees:	Controllers cannot charge a fee for complying with a request. (See 'general rules and exceptions')
Refusals:	Controllers may refuse to comply with all or part of the request for rectification but must be able to justify its decision. Requests may be refused in cases where: • the request is manifestly unfounded or excessive, in particular if it is repetitive (Art 12(5)); • a restriction on the right can be justified in the particular circumstances (Art 23)
Other points:	• Controllers should make it easy for data subjects to exercise their right (Art 12(2) & Rec 63) • Transparency information must include reference to this right

RIGHT TO ERASURE

"Right to erasure"

What the law says

Article 17

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay ***where one of the following grounds applies****:*

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

Article 19

"The controller shall communicate any … erasure of personal data … carried out in accordance with … Article 17(1) to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

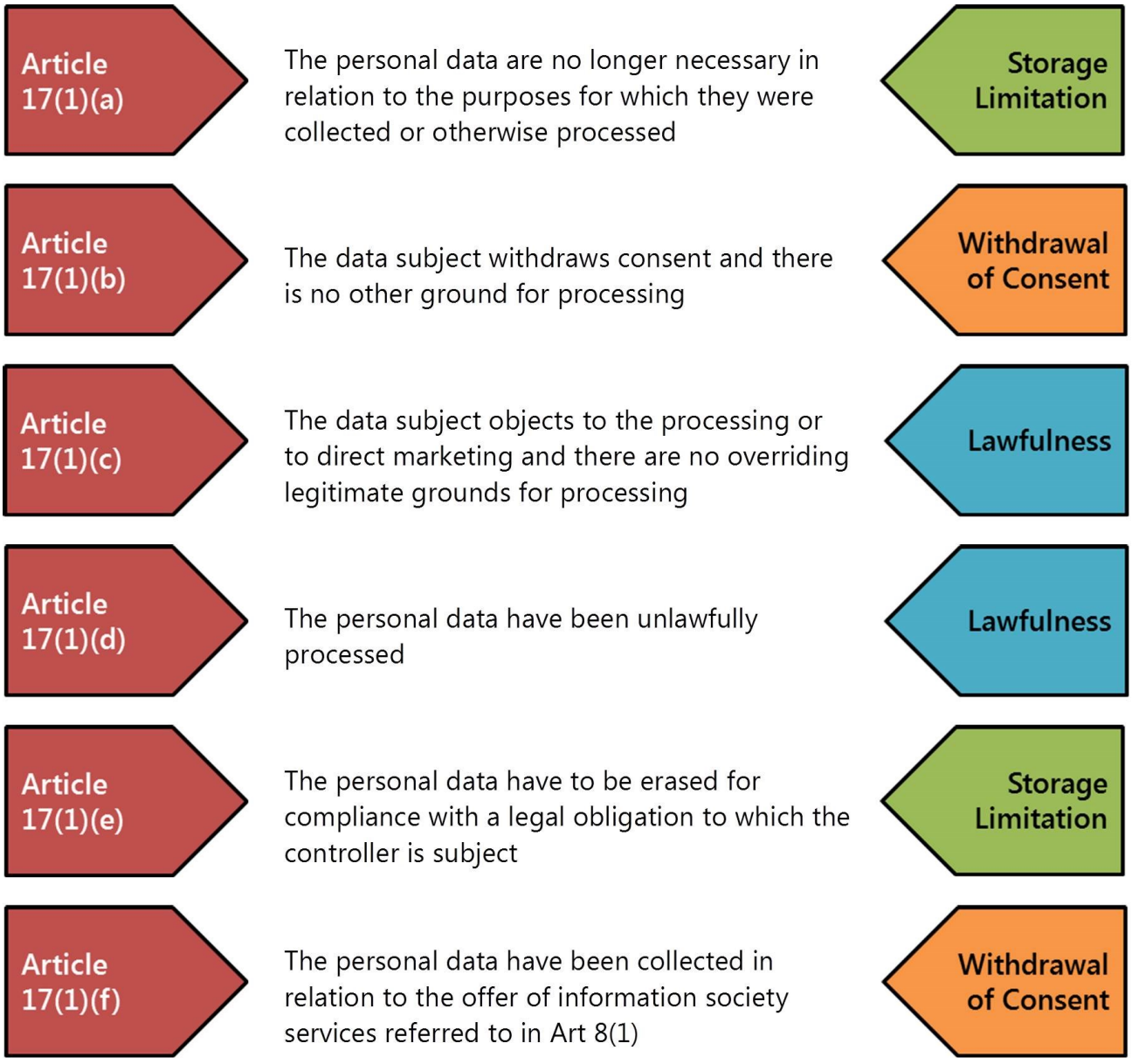
"Right to erasure"

- in practice

The right to erasure is also referred to as "the right to be forgotten". This right is not absolute and **can only be exercised in the circumstances specified in Article 17(1)** which are broadly equivalent to those set out in the right that already exists.

Those circumstances are also closely aligned with principles which impose obligations on controllers in respect of the processing of personal data. Compliance with the principles, including adherence to retention policies and understanding the grounds for processing, may, therefore, result in fewer erasure requests.

The following table lists the Article 17(1) grounds under which a request for erasure can be made and indicates the principle with which that right aligns.



"Right to erasure"

- in practice

Actions:	• **respond** to the individual to advise them on the action, or inaction, taken on their request; • **communicate** any actions to the individual; • **communicate** the erasure to each recipient it has been disclosed to (Art 19) • **inform** the data subject of the recipients if requested. (Art 19) • where the controller has made personal data, which it is obliged to erase, public, it must take reasonable steps to **inform** other controllers processing that personal data (e.g. links, copies etc.) of the requested erasure. (Art 17(2))
Timing:	Response must be without undue delay and at the latest within one calendar month (See 'general rules and exceptions').
Identification:	Controllers may take 'reasonable measures' to identify the person making the request. (See 'general rules and exceptions')
Fees:	Controllers cannot charge a fee for any communications or actions. (See 'general rules and exceptions')
Refusals:	Controllers may refuse to comply with all or part of the request for erasure but must be able to justify its decision. Requests may be refused in cases where: • none of the grounds in Article 17(1) apply; • a limitation on the right set out in Article 17(3) can be justified in the particular circumstances • the request is manifestly unfounded or excessive, in particular if it is repetitive • a restriction on the right can justified in the particular circumstances (Art 23)
Other points:	• Controllers should make it easy for data subjects to exercise their right (Art 12(2) & Rec 63) • Transparency information must include reference to this right

RIGHT TO RESTRICTION OF PROCESSING

"Right to restriction of processing"

What the law says

Article 18

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(c) 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;

(d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

2. Where processing has been restricted under paragraph 1, such 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.

Article 19

"The controller shall communicate any ... restriction of processing carried out in accordance with ... Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

"Right to restriction of processing" - in practice

This is a new right which gives individuals control over the use of their personal data in the form of the imposition of a restriction on further processing in four specified scenarios.

Article 4 defines restriction on processing as:

> *the marking of stored personal data with the aim of limiting their processing in the future*

Recital 67 suggests means by which processing can be restricted:

> *Methods by which to restrict the processing of personal data could include, inter alia, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website. In automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed.*

Recital 67 concludes:

> *The fact that the processing of personal data is restricted should be clearly indicated in the system.*

This appears to be intended to encourage the use of warnings or flags in systems to *'stop'* or *'proceed with caution'* if that personal data is being considered for processing whilst the restriction is in place.

Article 18(2) sets out the circumstances in which personal data can be processed by the controller during the term of a restriction.

These are

- for storage
- with the consent of the data subject
- for the establishment, exercise or defence of legal claims
- for reasons of important public interest of the Union or Member State

"Right to restriction of processing" - in practice

Individuals can exercise their right to restrict processing in the four scenarios set out in Article 18(1). Most of these scenarios align to compliance with a principle.

Therefore, the more effort a controller makes to be accountable and ensure processing complies with the principles (e.g. regular reviews of compliance with the principles and the grounds for processing), the more limited the circumstances may be in which this right could be exercised, and the lower the impact the exercise of the right may have on the controller.

The scenarios can be divided into **temporary** and **permanent** restrictions.

Temporary restrictions on processing

Temporary restrictions may be exercised in conjunction with other rights which require the controller to verify certain aspects of processing. The length of time that the restriction remains in place will depend on the time taken by the controller to make the relevant verification, subject to the Article 12 overriding duty to comply without undue delay and within one month.

1. Verification of accuracy

This restriction can be imposed by the individual to enable the controller to verify the accuracy of that data before any further processing occurs. It is not for the data subject to prove inaccuracy. Instead, it is explicitly the responsibility of the controller to verify the accuracy of the data before any further processing can occur. This aligns with the right to rectification of inaccurate data (Art 16) and the controller's duty to comply with the accuracy principle (Art 5(1)(d)).

2. Objection to certain grounds for processing

Where an individual has exercised their right to object to processing under Article 21(1) (see more under the Right to object to processing), the controller needs to restrict processing in order to verify whether or not its legitimate interests override those of the data subject. This aligns with the controllers duty to process personal data lawfully (Art 5(1)(a)).

Permanent restrictions on processing

The individual must be informed of the action taken in respect of the exercise of the right to permanent restrictions within the time frame set out in Article 12(3), i.e. without undue delay and within a month.

3. Unlawful processing

An individual can request a controller **not to erase** personal data that it is unlawfully processing even if the controller wishes to delete it.

The controller will need to establish whether the personal data is, or is not, being unlawfully processed before implementing a permanent restriction.

4. Required by the data subject for the establishment, exercise or defence of legal claims

An individual has the right to prevent a controller processing (including erasing) personal data which that individual requires for legal proceedings, even if the controller has no purpose for processing, or holding, that data itself. Controllers will, therefore, need to communicate with the individual and establish that the data is required for such a purpose when such a restriction of processing is received.

"Right to restriction of processing"

Actions:	• **respond** to the individual to advise them on the action, or inaction, taken on their request; • **communicate** any actions to the individual; • **communicate** the restriction to each recipient it has been disclosed to (Art 19) • **inform** the data subject of the recipients if requested. (Art 19) • **inform** the data subject prior to lifting the restriction (Art 18(3))
Timing:	**Restrictions** must be complied with without undue delay and at the latest within one calendar month (See 'general rules and exceptions').
Identification:	Controllers may take 'reasonable measures' to identify the person making the request. (See 'general rules and exceptions')
Fees:	Controllers cannot charge a fee for any communications or actions. (See 'general rules and exceptions')
Refusals:	Controllers may refuse to comply with all or part of the request for restriction but must be able to justify its decision. Requests may be refused in cases where: • none of the grounds in Article 18(1) apply or can be established; • the request is manifestly unfounded or excessive, in particular if it is repetitive; • a restriction on the right can be justified in the particular circumstances (Art 23)
Other points:	• Controllers should make it easy for data subjects to exercise their right (Art 12(2) & Rec 63) • Transparency information must include reference to this right

RIGHT TO DATA PORTABILITY

"Right to data portability"

What the law says

Article 20

1. *The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine -readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:*

   (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and

   (b) the processing is carried out by automated means.

2. *In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.*

3. *The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to 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.*

4. *The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.*

The Article 29 Working Party has adopted guidance on the right to data portability which should be referred to for further information.

This is available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=44099

In summary, the right applies only to personal data:

- Supplied by the individual to the controller; and
- Processed with the consent of the individual or under the terms of a contract; and
- Processed by automated means

It does not apply to personal data which is necessarily being processed to comply with a legal obligation or in the exercise of public duties.

"Right to data portability"

What the law says

Recital 68

To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller.

Data controllers should be encouraged to develop interoperable formats that enable data portability.

That right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It should not apply where processing is based on a legal ground other than consent or contract.

By its very nature, that right should not be exercised against controllers processing personal data in the exercise of their public duties. It should therefore not apply where the processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller.

The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible.

Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation.

Furthermore, that right should not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in this Regulation and should, in particular, not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract to the extent that and for as long as the personal data are necessary for the performance of that contract.

Where technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another.

"Right to data portability"

Actions:	• **respond** to the individual to advise them on the action, or inaction, taken on their request; • **communicate** any actions to the individual;
Timing:	Response must be without undue delay and at the latest within one calendar month (See 'general rules and exceptions').
Identification:	Controllers may take 'reasonable measures' to identify the person making the request. (See 'general rules and exceptions')
Fees:	Controllers cannot charge a fee for any communications or actions. (See 'general rules and exceptions')
Refusals:	Controllers may refuse to comply with all or part of the request for restriction but must be able to justify its decision. Requests may be refused in cases where: • The criteria set out in Article 20(1)(a) & (b) are not met • the request is manifestly unfounded or excessive, in particular if it is repetitive; • a restriction on the right can be justified in the particular circumstances (Art 23)
Other points:	• Controllers should make it easy for data subjects to exercise their right (Art 12(2) & Rec 63) • Transparency information must include reference to this right

RIGHT TO OBJECT

"Right to object"

What the law says

Article 21

1. *The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.*
2. *Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.*
3. *Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.*
4. *At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.*
5. *In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.*
6. *Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.*

"Right to object"

There are two circumstances where the right to object to processing can be exercised:

1. An absolute right to object to processing for the purposes of direct marketing (Art 21(2) & (3))
2. Qualified general rights in specified circumstances (Art 21(1) & (6))

1. The absolute right to object to processing for direct marketing purposes

This right is similar to the existing right and continues to apply to ANY form of marketing. Controllers should note that whilst there continue to be additional specific rules relating to electronic direct marketing, these do not form part of this advice note.

New elements mean that the right:

- applies to profiling of individuals undertaken in respect of direct marketing activities; and
- must be brought explicitly to the attention of individuals.

Article 21(4) re-emphasises the transparency obligations under **Article 12(1)** and requires controllers to bring details of these rights to the attention of individuals:

- "explicitly"
- "at the latest at the time of the first communication"
- "clearly and separately from any other information"

Recital 70 states:

> *Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge. That should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information.*

Article 17(1)(c) provides a corresponding **right to erasure** which can be exercised where processing is only for the purposes of **direct marketing**.

"Right to object"

2. Qualified general rights in specified circumstances

- **Article 21(1)**

Individuals have the right to object to all, or particular, elements of processing, such as disclosures to certain parties, including for profiling purposes, where the processing is necessary for one of two specific grounds:

- The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- the purposes of legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

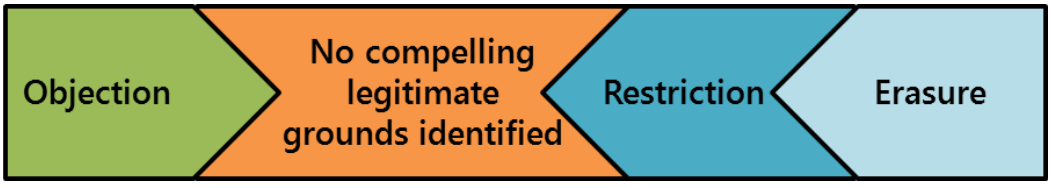
Recital 69 states:

> *Where personal data might lawfully be processed because processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or on grounds of the legitimate interests of a controller or a third party, a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation. It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject.*

In the case of public interest tasks etc., these are discretionary exercises of official authority, or implied powers, and is of particular relevance to the public sector. The legitimate interest ground for processing only applies in the private sector. In either case, controllers must make a specific consideration of the processing of that individual's personal data in the context of their particular circumstances. It cannot be a generalised deliberation.

The controller **cannot process** the relevant personal data until **it has demonstrated** "compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims".

Where a controller cannot demonstrate compelling legal grounds, other rights, including the Article 17(1)(c) right to erasure and the Article 18(1)(d) restriction on processing explicitly apply if exercised.



"Right to object"

- **Article 21(6)**

This provides a limited qualified right for an individual to object to the processing of their personal data for research or statistical purposes. This only applies if that research or statistical information is 'personal data' which has not been anonymised to prevent the identification of the individual.

This objection must be based on grounds relating to the **particular situation of the individual**.

The right can, however, be overridden if the processing is necessary for the performance of a task carried out for reasons of public interest. Although there is no explicit provision in Article 21 relating to a controller demonstrating the necessity of the processing when considering such an objection to processing, there is the overriding obligation in Article 5(2) for controllers to demonstrate compliance with the principles (accountability). This includes meeting an Article 6 ground for lawful processing which, with the exception of consent, requires the processing to be "necessary".

"Right to object"

Actions:	• **respond** to the individual to advise them on the action, or inaction, taken on their request; • **communicate** any actions to the individual;
Timing:	Response must be without undue delay and at the latest within one calendar month (See 'general rules and exceptions').
Identification:	Controllers may take 'reasonable measures' to identify the person making the request. (See 'general rules and exceptions')
Fees:	Controllers cannot charge a fee for any communications or actions. (See 'general rules and exceptions')
Refusals:	Controllers may refuse to comply with all or part of the request for restriction but must be able to justify its decision. Requests may be refused in cases where: • The criteria set out in Article 21(1),(2) or (6) are not met • the request is manifestly unfounded or excessive, in particular if it is repetitive; • a restriction on the right can be justified in the particular circumstances (Art 23)
Other points:	• Controllers should make it easy for data subjects to exercise their right (Art 12(2) & Rec 63) • Transparency information must include reference to this right • Article 21(5) permits individuals to exercise use automated means to object to the processing of their personal data by 'information society services' for one of the reasons set out in Article 21. (The definition of 'information society services' is included in the Definitions Closer Look guide)

RIGHTS IN RELATION TO AUTOMATED PROCESSING, INCLUDING PROFILING

Rights in relation to "Automated individual decision-making, including profiling"

What the law says

Article 22

1. *The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.*

2. *Paragraph 1 shall not apply if the decision:*

   (a) is necessary for entering into, or performance of, a contract between the data subject and a controller;

   (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

   (c) is based on the data subject's explicit consent.

3. *In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.*

4. *Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.*

Rights in relation to "Automated individual decision-making, including profiling"

Profiling and automated decisions are increasingly prevalent in the private and public sectors. Examples of automated decisions include credit-scoring, insurance premium calculations, psychometric testing. Individuals are accustomed to some profiling, for example through the use of store loyalty cards and online advertising. Technological advances, including data analytics, the Internet of Things (IoT), artificial intelligence (AI) etc., have also increased the capacity for profiling to occur and opened up greater uses for that data.

Automated decisions (including automated profiling) can benefit businesses and individuals, but can also pose significant risks for individuals in relation to their fundamental rights and freedoms. GDPR balances these two competing interests by giving individuals the right to object to decisions being taken about them based solely on automated processing (including automated profiling) which evaluate personal aspects relating to them.

Recital 71 provides further insight as to what processing is covered by this right:

> *"any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her."*

This right is, however, restricted to processing which will result in "legal effects concerning him or her or similarly significantly affects him or her". Where such effects do not result from the automated processing, individuals have other rights they may exercise, such as the right to object to processing.

The right to not be subject to automated decision-making **cannot be exercised** where the controller is making a decision which is:

- authorised by law;
- necessary for entering into, or performance of, a contract with the individual; or
- based on explicit consent (Article 9(2) i.e. special categories of personal data).

Where the automated decision is in connection with a contract (for example, automated credit scoring in connection with a loan application) or based on explicit consent, the controller must ensure that the data subject's rights, freedoms and legitimate interests are protected. These safeguards must include *"the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision"* (Art 22(3)).

In addition, controllers must ensure that the processing of personal data for making automated decisions complies with all the requirements of the GDPR, in particular Articles 5 & 6, principles and grounds for processing.

Rights in relation to "Automated individual decision-making, including profiling"

Actions:	• **respond** to the individual to advise them on the action, or inaction, taken on their request; • **communicate** any actions to the individual;
Timing:	Response must be without undue delay and at the latest within one calendar month (See 'general rules and exceptions').
Fees:	Controllers cannot charge a fee for any communications or actions. (See 'general rules and exceptions')
Refusals:	Controllers may refuse to comply with the right but must be able to justify its decision. The exercise of the right may be refused in cases where: • the processing does not result in effects set out in Article 22(1) or the processing is based on one of the criteria set out in Article 22(2); • the request is manifestly unfounded or excessive, in particular if it is repetitive; • a restriction on the right can be justified in the particular circumstances (Art 23)
Other points:	• Controllers should make it easy for data subjects to exercise their right (Art 12(2) & Rec 63) • Transparency information must provide meaningful information about the logic involved and the significance and envisaged consequences of the processing for the individual. (Art 13(2)(f))

REMEDIES

REMEDIES

Individuals have several remedies against controllers or processors if they consider that their rights have been breached or there is non-compliance with the requirements of the law.

These remedies can be sought without prejudicing any other action or remedy.

The remedies of complaint to the supervisory authority, to take court action against the controller and to seek compensation from the controller are substantially similar to those currently in force.

However, for the first time, in some circumstances these remedies can be exercised against PROCESSORS as well as controllers (This does not include compliance with rights).

There is also a significant new remedy set out in Article 80 that allows individuals to give authority to a third party to act on their behalf in the seeking a remedy against a controller or processor. Such a third party must be properly constituted not-for-profit body, organisation or association, with objectives in the public interest, and active in the field of the data protection. Those third parties can also act on behalf of a data subject in respect of a claim for compensation under Article 82.

Article 80 also opens up the possibility for Member States to introduce law to allow for 'class actions' to be taken by such third parties, irrespective of whether they have been asked to take action by a particular data subject(s).

The ability to appoint a specified type of third party under Article 80, does not, in any event, stop an individual from engaging a lawyer or advocate to act on their behalf when exercising either their rights or seeking remedies.

REMEDIES

What the law says:

Article 77: Right to lodge a complaint with a supervisory authority

1. *Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.*

2. *The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78 [against a supervisory authority or the European Data Protection Board].*

Article 79: Right to an effective judicial remedy against a controller or processor

1. *Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.*

2. *Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.*

REMEDIES

What the law says:

Article 80: Representation of data subjects

1. *The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.*

2. *Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.*

Article 82: Right to compensation from controllers and processors

1. *Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.*

2. *Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.*


information
commissioner
Barrantagh Fysseree