Subject access, rectification and portability

At a glance

- Data controllers must, on request:
  - confirm if they process an individual's personal data;
  - provide a copy of the data (in commonly used electronic form in many cases); and
  - provide supporting (and detailed) explanatory materials.
- Data subjects can also demand that their personal data be ported to them or a new provider in machine readable format if the data in question was: 1) provided by the data subject to the controller (interpreted broadly); 2) is processed automatically; and 3) is processed based on consent or fulfilment of a contract.
- The request must be met within one month (with extensions for some cases) and any intention not to comply must be explained to the individual.
- Access rights are intended to allow individuals to check the lawfulness of processing and the right to a copy should not adversely affect the rights of others.

To do list

☐	Review customer facing team's processes, procedures and training – are they sufficient to deal with the GDPR's access and portability rules?
☐	Develop template response letters, to ensure that all elements of supporting information are provided.
☐	Assess your organisation's ability to provide data in compliance with the GDPR's format obligations. It may be necessary to develop formatting capabilities to meet access requests.
☐	If portability applies, consider which of your records are covered by this. Check if the data (and associated meta data) can easily be exported in structured, machine-readable formats. Look out for industry initiatives to develop interoperable formats.
☐	Consider developing data subject access portals, to allow direct exercise of subject access rights.

Right of information and access

An individual has the following rights with regards to a data controller:

- to obtain confirmation whether his/her personal data are being processed;
- to access the data (i.e. to a copy); and
- to be provided with supplemental information about the processing.

As with all data subject rights, the controller must comply *"without undue delay"* and *"at the latest within one month"*, although there are some possibilities to extend this.

The controller must also use reasonable means to verify the identity of the person making the request – but should not keep or collect data just so as to be able to meet subject access requests. These points are particularly pertinent to online services.

Right of access to data

The controller must provide *"a copy of the personal data undergoing processing"*. This must be provided free of charge (a change for UK based controllers), although the controller may charge a reasonable, administrative-cost fee, if further copies are requested.

If the request is made in electronic form, the information should be provided in a commonly used electronic form (unless the data subject requests otherwise). This could impose costs on controllers who use special formats, or who hold paper records.

Recital 63 also suggests that, where possible, the controller may provide a secure system which would grant the data subject direct access to his/her data. This seems to be encouraged rather than required.

Supplemental information

The controller must also provide the following information (the items in italics are not currently mandated by the Data Protection Directive – although they are required under some Member State laws implementing the Data Protection Directive):

- the purposes of processing;
- the categories of data processed;
- the recipients, or categories of recipients *(in particular, details of disclosure to recipients in third countries or to international organisations* (bodies governed by public international law or set up by agreement between countries));
- *the envisaged retention period, or, if this is not possible, the criteria used to determine this period;*
- *the individual's rights of rectification or erasure, to restrict processing or to object to processing and to lodge a complaint to a supervisory authority;*
- *information regarding the source of the data (if not collected from the data subject);*and
- any regulated automated decision taking (i.e. decisions taken solely on an automated basis and having legal or similar effects; also, automated decision taking involving sensitive data) – including information about the logic involved and the *significance and envisaged consequences of the processing for the data subject.*

If the controller does not intend to comply with the request, he must also provide reasons.

Exemptions

The GDPR recognises that subject access may adversely affect others and provides that the right to receive a copy of the data shall not adversely affect such rights. Recital 63 notes that this could extend to protection of intellectual property rights and trade secrets (for example, if release of the logic of automated decision taking would involve release of such information). However, the recital also notes that a controller cannot refuse to provide *all* information, on the basis that access may infringe others' rights.

Recital 63 also contains two other useful limiting provisions:

- if the controller holds a large quantity of data, it may ask the data subject to specify the information or processing activities to which the request relates. (However, the recital does not go on to say that there is any exemption due to large volumes of relevant data: the limitation seems to be more to do with the specificity of the request, rather than the extent of time and effort on the controller's part – although the two may, of course, be linked);
- the data subject's right is *"to be aware of and verify the lawfulness of the processing".* This confirms the comments made by the CJEU in *YS v Minister voor Immigratie, Integratie en Asiel* (Case C-141/12) that the purpose of subject access requests is to allow the individual to confirm the accuracy of data and confirm the lawfulness of processing and to allow them to exercise rights of correction or objection etc if necessary. In other words, the purpose is related to the individual's rights under data protection legislation: requests made for other, non-data protection purposes, may possibly be rejected.

Rectification

Individuals can require a controller to rectify inaccuracies in personal data held about them. In some circumstances, if personal data are incomplete, an individual can require the controller to complete the data, or to record a supplementary statement.

Portability

The subject access right provided under the GDPR already gives individuals the right to require their data to be provided in a commonly used electronic form.

Data portability goes beyond this and requires the controller to provide information in a structured, commonly used and machine readable form so that it may be transferred by the data subject to another data controller without hindrance. Further, the controller can be required to transmit the data directly to another controller where it is technically feasible to do so. The GDPR encourages controllers to develop interoperable formats.

Whereas subject access is a broad right, portability is narrower. It applies:

- to personal data which is processed by automated means (no paper records);
- to personal data which the data subject has provided to the controller; and
- only where the basis for processing is consent, or that the data are being processed to fulfil a contract or steps preparatory to a contract.

Data which the individual "has provided" is interpreted widely. Pursuant to guidance from the Article 29 Working Party, this is not limited to forms completed by an individual, but to information gathered by the controller in the course of its dealings with the individual or generated from observation of his or her activity. Examples of occasions when data portability will apply include: (i) data held by a music streaming service, (ii) titles of books held by an online bookstore, (iii) data from a smart meter or other connected objects, (iv) activity logs, (v) history of website usage, (vi) search activities or (vii) emails sent to the individual. However, the portability right does not extend to personal data which is inferred or derived by the data controller (for example, the results of an algorithmic analysis of an individual's behaviour).

Whilst data portability applies only to data controllers, data processors will be under contractual obligations to assist controllers "by appropriate technical and organisational measures" with responding to portability requests. Data controllers should therefore implement specific procedures with their processors on handling such requests.

Data portability must not prejudice the rights of other individuals. However, according to data protection authorities, the original data controller is not responsible for the receiving the data controller's compliance. Instead, any organisation receiving the data must ensure that its use of the data is lawful.

There are exemptions from portability - for example, where this would adversely affect IPRs or trade secrets. Data protection authorities consider that this does not excuse all compliance with the right.

Data portability requirements may also conflict with other access and portability requirements in sector-specific EU (e.g. the right to access one's bank account history under the Payment Services Directive 2) or member state legislation. Guidance from the Article 29 Working Party explains that the GDPR portability right will not apply if the individual makes clear he is exercising his rights under another law. If, however, the individual seeks to exercise his rights under the GDPR, the controller must assess the interplay between any competing rights case-by-case, but the more specific legislation will not automatically displace the GDPR right.

Where can I find this?

Subject access	*Article 15*	*Recitals 59, 63, 64*
Rectification	*Article 16*	*-*
Portability	*Article 20 and WP 242*	*Recital 68*