The Rights of Data Subjects

What Rights Are Available to Data Subjects?

One of the main focuses of the GDPR legislation is protecting the rights and freedoms of data subjects, especially in relation to their personal data. To do this, there are eight rights that are directly mentioned. These allow subjects to have a more comprehensive understanding of their data, as well as increased control.

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Right to avoid automated decision-making

The Right to Be Informed

The **right to be informed** covers the organisation's necessity to provide fair processing information, with an emphasis on transparency. Privacy notices are often used as a way to inform data subjects about their rights.

A data subject is entitled to know:

- what personal information of theirs is being processed
- the lawful basis of the processing
- whether their data will be processed by the controller or a third party
- the purposes of processing, and how long it will be kept

Organisations need to ensure their practices meet the requirements for transparency. They also need to ensure data subjects are aware of their right to complain to the ICO, which is outlined in Article 77 of the GDPR regulation. This information must be included in the medium used to provide privacy information.

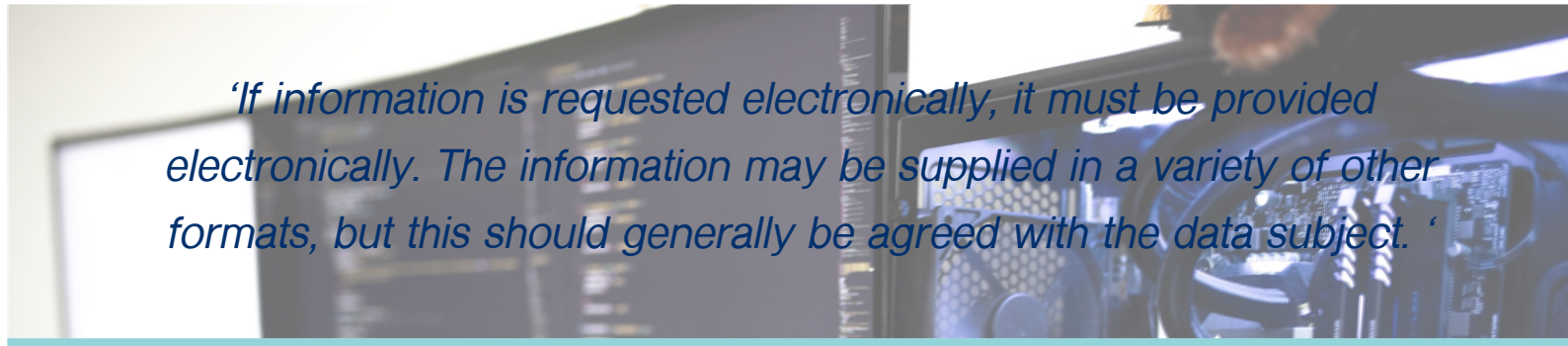
'Organisations must provide privacy information to data subjects at the time that their personal data is collected. If this is obtained from elsewhere, it must be provided within a month.'

The ICO provides a list of techniques that organisations can use to provide people with privacy information, including:

- a layer approached approach: short notices containing key privacy info that have layers with more details
- dashboards – preference management tools that inform people how you use their data and allow them to manage it
- just-in-time notice – relevant and focused privacy information at the time of collection
- icons – small, meaningful symbols that indicate the existence of a particular type of data processing
- mobile and smart devices functionalities – including pop-ups, voice alerts, and mobile device gestures

'The information provided to subjects must be, oncise, transparent, understandable, and easily accessible. It must also be communicated in clear and plain language and free to access'.

'Know your rights'



'If information is requested electronically, it must be provided electronically. The information may be supplied in a variety of other formats, but this should generally be agreed with the data subject. '

The Right of Access

Article 15 of the GDPR stipulates that the data controller must give data subjects access to the personal data the organisation holds on them, as well as confirmation of any processing involving their data and any other supplementary information.

It should be noted that not all personal data is covered under the regulation, and if an individual makes unfounded or excessive requests, the controller has the right to refuse any information request, or to charge a reasonable fee to cover the resulting administrative costs. The data subject must also be informed within at least one month of receipt of the request, with the reasons for not taking action.

If the request is rejected or a response is refused, the data subject is entitled to adequate reasoning explaining why this is the case. They must also be informed about their rights to contact the Information Commissioner's Office.

The mechanism that allows data subjects to make requests for their data is called a subject access request (SAR). Subject access requests may be made in writing, including via email or verbally, and must be considered a valid request regardless of its format.

Responding to a subject access request firstly requires the identity of the individual making the request to be verified. Verification may be sought through having sight of the data subject's passport or photo driving license to confirm their identity, which would be reasonable and an appropriate means of verification.

The Right to Rectification

Under Article 16 of the GDPR regulation, the data subject has the right to rectify any inaccuracies in the personal data held about them. Inaccurate data includes incomplete data, so data subjects can also request that the data controller completes any partial data, which might be achieved by providing the data controller with a supplementary statement. Any third parties should be updated of the correction.

If an organisation receives a complaint of inaccurate data, then they must take reasonable steps to fix the situation. The nature of the personal data will help to determine the response required. The more vital that the personal data is accurate, the greater effort needs to be exerted when checking its accuracy, If the data will be used to make significant decisions that may affect the subject themself or other, then the organisation has a greater duty to ensure that this is rectified. Organisations should keep a record of any mistakes made for transparency.

As the right of rectification is closely linked to the right of access, it would be sensible to link the processes used to support these two rights. For instance, if data subjects will be their personal data online, you might use the same web interface to allow them to edit their personal data.

'An organisation has one month to respond to any complaints of inaccurate data, unless there are reasons to extend by up to another two months, in which case a reasonable explanation will be required.

'The right to erasure is often known as the right to be forgotten. Under Article 17, data subjects can request that information be erased and ask that any further processing in specific situations be prevented.'

Recital 65 of the GDPR states that if an organisation processes any personal data of children, they should pay special attention to existing situations where a child has already given consent and later requested erasure, as the child may not be aware of the risks when giving consent initially. '

The Right to Erasure

Organisations can refuse a request for erasure where the personal data is being processed for the following reasons:

- to protect the right of freedom of expression and information
- to comply with a legal obligation for the performance of a public interest task
- exercise of official authority
- for public health reasons
- for archiving purposes in the public interest, historical or scientific research purposes,
- exercise or defense of a legal claim

It is important to note that the right to erasure is **not absolute**, and only applies in particular circumstances:

- when the personal data is no longer necessary for the purpose for which they were collected
- if the data subject withdraws consent to processing, assuming there is no other legal justification for processing
- if the data subject object to processing based on legitimate interests and the data controller cannot demonstrate an overriding legitimate ground for the processing
- if the data has been unlawfully processed, in breach of GDPR

There are, however, additional requirements when it comes to the erasing of personal data relating to children. These additional requirements emphasise that there must be enhanced protection of such information, especially in online environments.

The Right to Restrict Processing

Organisations should restrict processing of personal data in the following circumstances:

- where the accuracy of the personal data is contested
- if the personal data is no longer needed
- when processing is unlawful
- when they object to their data being processed under the right to object, whilst the organisation investigates the legitimacy of the claim
- if the organisation needs to review procedures to make sure they can determine where restrictions may be needed

GDPR suggests a few ways for organisations to restrict processing:

- moving the data to another processing system as a temporary measure
- making the data unavailable to users
- temporarily removing published data from a website

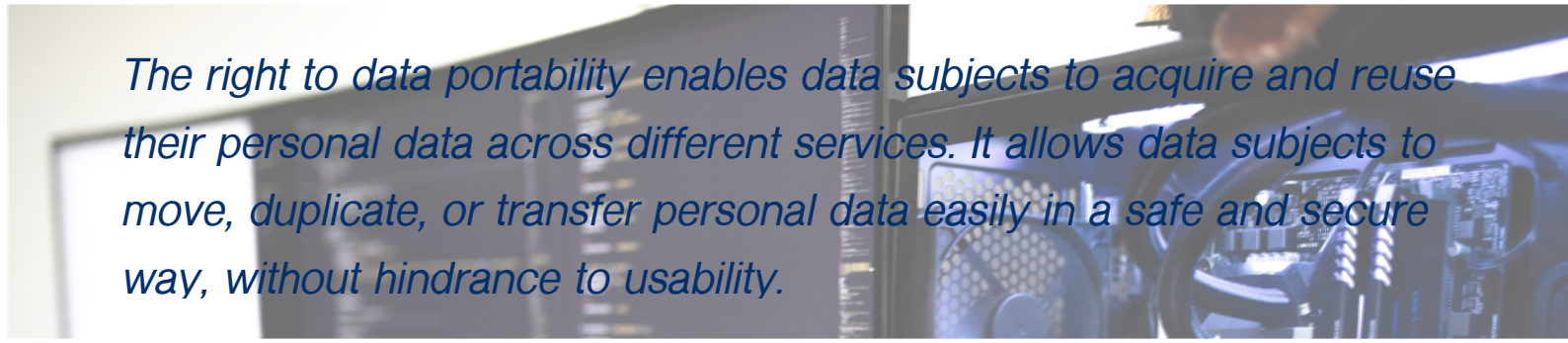
Article 18 states that if a subject requests that processing of their personal data be restricted, the organisation may store it, but can't process it further. Organisations should retain enough information to guarantee that this restriction can be continued.

The Right of Data Portability

The right of data portability only applies to personal data that an individual has provided to a data controller, where the processing is based on the individual's consent, or when processing is carried out by automated means.

When a request for data portability comes in, it is essential that the organisation provides the data in an organised, frequently used, and suitable format, for example a CSV file.

'If data has been disclosed to third parties, they must be notified as soon as possible. This can be forgone if this isn't a possibility, or it involves disproportionate effort to do so. '



The right to data portability enables data subjects to acquire and reuse their personal data across different services. It allows data subjects to move, duplicate, or transfer personal data easily in a safe and secure way, without hindrance to usability.

Organisations may, at the request of the data subject, directly transmit the data to another organisation but only if it is technically feasible. It is not a requirement of the regulation to adopt, provide or maintain processing systems that are technically compatible with those of other organisations. This information, should a data subject put in a request for the transfer of their data, must be provided free of charge.

The Right to Object

Article 21 of the GDPR gives individuals the right to object to having their personal data processed. Effectively, they can prevent organisations from processing their data. The objection can be about all the information held about a person, or just specific information. When an organisation receives a complaint, the processing in question must stop, and it is the burden of the controller to provide legitimate grounds as to why that the processing overrides the rights and freedoms of the subject in question.

Data subjects can object to specific types of processing, for example processing in the wider public interest, or direct marketing. If a data subject opposes their data being used for direct marketing, companies must comply immediately, with no exceptions or arguments. If a subject objects to their data being used for scientific purposes, then they must object on the grounds 'relating to his or her specific situation'. In this case, compliance is not a given as the value of the research in the public interest outweighs the rights of any one individual. Organisations can also refuse to comply if the request is unfounded or excessive, but you must be able to demonstrate why you refused the request.

Objections can be written or verbal – there is no set way for an individual to object to their data being processed. Data subjects must also be informed of their right to object when they are first in contact with the organisation. This information must be given to subjects 'clearly and separately from any other information', and where services are online, there has to be an automated way for subjects to exercise this right. Controllers are obliged to prove the need for the data processing they are approving in order to assure that subjects are given adequate notice of their rights.

The Right to Avoid Automated Decision-Making

GDPR introduced safeguards to protect against the possibility that a harmful decision can be made without human intervention, and safeguards surrounding profiling, which is automated processing of personal data to evaluate things about a subject. Individuals possess the right not to be subject to an agreement that is focused on automated processing.

Automated decision making can only be carried out when the decision is;

- necessary for the entry into/performance of a contract
- authorised by domestic law applicable to the controller (e.g. for fraud purposes)
- based on an individual's explicit consent

If the decision making includes special category person data, then you can only carry out processing if;

- you have the explicit consent of the individual
- it is necessary for reasons of public interest

Organisations must have safeguards in place when they are using data for the purposes of profiling. If an organisation's processing activities fall under this category, then they must:

- give subjects information about the processing
- introduce simple ways for them to challenge a decision and/or request human intervention
- carry out regular checks to make sure that systems are in full working order

in order to gain consent for automated processing, organisations must make it very clear what is involved.

shardbusiness
07714651415
www.shardbusinessservices.co.uk
@shardbusiness
sheryl-cardwell-fisbl
office@shardbusinessservices.co.uk