

INTRODUCTION TO THE RIGHTS OF DATA SUBJECTS

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



TO HAVE 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.

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

Responding to a SAR 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.

TO BE INFORMED

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

KNOW YOUR RIGHTS

'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.

TO HAVE DATA ERASED

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

RIGHTS OF DATA SUBJECTS

TO 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.

TO RECTIFY

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.

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.

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

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



shardbusinessservices.co.uk



07714651415



office@shardbusinessservices.co.uk



shardbusinessservices



shardbusiness



@shardbusiness