

## Right of access how to implement it



The General Data Protection Regulation (GDPR) gives individuals greater control over their personal data by granting them a series of data subject rights.

One such important right is **the right of access**, which allows individuals to **request access to the personal data organisations hold about them**. The aim of this right is to empower individuals to verify the legality and accuracy of the data processed about them. This will make it easier for individuals to exercise other rights such as the right to erasure or rectification.

The [EDPB guidelines on data subject rights - right of access](#) analyse the various aspects of the right of access and provide precise and practical guidance on how to implement it in different situations.

↓ The right of access includes **three main components**:

### 1 Confirmation whether individuals' personal data are being processed

When individuals request access to their personal data, it is important that organisations **first check if they have any data about the requester**. If not, they can simply confirm that no data are processed. If they do have data, they should confirm this.

### 2 Access to the personal data held about individuals

When individuals request access to their personal data, they should receive the **actual data**, not just summaries. They have the right to access all or part of their data, regardless of its type or source, to understand how it is used. It is key that organisations ensure the information is **complete, accurate, and up-to-date** at the time of the request.

### 3 Access to detailed information about the data processing, including its purpose, the types of data involved, the recipients, the duration of processing, their rights as individuals, and the safeguards in place for transfers to third countries

Organisations should **inform individuals how their data are processed and what rights they have**. They can do so via a privacy notice or processing records (documented log of personal data processing activities within an organisation). The information should be updated and tailored to each request.

## Granting data access on time

It is important that organisations respond without undue delay and at the latest **within one month after receiving the request for data access**. This deadline can be **extended by another two months** if the request is complex and more time is needed to answer, but in that case the individual should be informed of this within one month after the request has been received.

## No formal requirements and no need for justification

There are no specific requirements on the format of a request and no need to justify the request. While no formal format is required by law, the EDPB encourages organisations to provide for appropriate and user-friendly communication channels that can easily be used by the individual. If the individuals use a different point of contact, such as their usual point of contact within the organisation, their request should be redirected to the right place.

Organisations may choose, depending on the situation, to provide the copy of the data together with the supplementary information (please refer to point 3 above) in different ways, e.g. by **e-mail, physical mail or by the use of a self-service tool** (tool enabling users to access their data on their own, without support from the organisation). Adequate security measures, including possibly encryption, should protect the communication of this data.

### EXAMPLE 1



#### Context

A local bookstore keeps a record of names and addresses of their customers that have ordered home delivery. A customer visits the bookstore and makes a request for access.

→ In this situation, it would be sufficient to print out the personal data concerning the customer directly from the business system, while also supplying the supplementary information.

### EXAMPLE 2



#### Context

A monthly donor to a charity organisation makes an access request via e-mail. The charity organisation holds information about donations made in the past twelve months, as well as names and e-mail addresses of the donors.

→ The organisation could provide the copy of the personal data and the supplementary information by responding to the e-mail.

### EXAMPLE 3



#### Context

A social media service has an automated process for handling access requests in place that enables individuals to access their personal data from their user account.

→ To retrieve their personal data, the social media users can choose the option to “Download your personal data” when logged into their user account. This self-service option allows the users to download a file containing their personal data directly from the user account to their own computer.

## First copy of personal data provided at no cost

The first copy of the personal data processed must be provided free of charge, even if organisations consider the cost of reproduction to be high.

## Sending personal data to the right person

To protect individuals' personal data and avoid sharing it with the wrong people, **organisations should be able to find out which data refer to the individual making the request (identification) and confirm the identity of that person (authentication).**

If the organisation has reasonable doubts concerning the identity of the individual making the request, it may request additional information to confirm the identity of the person. However, organisations cannot request more personal data than is necessary to enable this authentication, and the use of such information should be strictly limited to fulfilling the individual's request.

## Possible restrictions

When someone asks for a copy of their data, **the rights of others need to be taken into account.** Other individuals' privacy rights should be considered, as well as trade secrets, intellectual property, and software copyrights. In practice, organisations should therefore consider if some information should be redacted, and this limitation should not be used as a reason to withhold all information from the individual requesting it.

### EXAMPLE 1



#### Context

An individual, who is now an adult, was cared for by the youth welfare office over a number of years in the past. The files about this period may possibly contain sensitive information about other persons (parents, social workers, or other minors).

→ The youth welfare office should carefully check if the rights and freedoms of others are affected. Depending on the result, some information may be redacted, such as names.

In case of manifestly unfounded or excessive (repetitive) requests for the right of access, organisations can refuse to comply with such requests or charge a reasonable fee. However, this assessment should be done carefully to ensure that transparency and free rights for individuals are preserved. Organisations must explain to the individual why they think the request is unreasonable or excessive, and if asked, provide reasons to Data Protection Authorities.

## Data access requests on behalf of another person

Although the concerned individual generally exercises the right of access, it is possible for a third party to make a request on behalf of another person. This may apply for instance to legal guardians acting on behalf of minors.

 [Read the guidelines](#)

This document presents a simplified version of the examples included in the guidelines. Please refer to the full examples in the original guidelines before taking a decision on similar cases for important implementation details and needed additional safeguard.