

# Form for making a subject access request (compliant with the GDPR)

## When to use this model subject access request form

The subject access request form allows individuals to request to their personal data.

## Form wording

The wording in this document reflects the requirements of the General Data Protection Regulation (GDPR), which will come into effect in the UK on 25 May 2018.

## Law relating to this document

### Leading statutory authority

General Data Protection Regulation (2016/679 EU)

The General Data Protection Regulation (GDPR) allows individuals to access information from organisations that process their personal data. The process for obtaining this information is known as a subject access request (sometimes referred to as a SAR or DSAR). It is common for employees or former employees to make subject access requests in the context of actual or threatened employment-related litigation or employment-related grievances.

In response to a subject access request, employers must provide the following information:

- whether or not the individual's personal data is being processed;
- the purposes of the processing and the categories of personal data concerned;
- the recipients to whom the data has been or will be disclosed, including recipients in countries outside the European Economic Area and the appropriate safeguards relating to such data transfers;
- for how long the data will be stored, or how that period is determined;
- the individual's rights in relation to the rectification or erasure of data, the restriction of processing and to object to processing;
- the individual's right to lodge a complaint with the supervisory authority;
- any third-party sources of the data, where this information is available; and
- information about the logic involved in any automated decision-making, if applicable.

The employer is also required to provide the individual with a copy of the personal data undergoing processing. If the subject access request is made electronically, the information has

to be provided in a commonly used electronic format, unless the individual agrees to receive it in some other way.

Individuals can make a subject access request through any format. However, an organisation can provide a form to assist individuals with making a request and to streamline the process for responding to a subject access request. Employers have a positive obligation to facilitate data subject rights under the GDPR, including an individual's right to access his or her personal data.

Organisations are not required to comply with a subject access request if they cannot identify the individual. Employers may also need to verify the individual's identity to ensure that personal data is not inadvertently disclosed to a third party. As a result, employers sometimes need to ask for identification to check that a request is from a particular individual. This is less likely in the context of an ongoing employment relationship: if an employer receives an internal subject access request from one of its existing employees, it may be unreasonable to ask for proof of identity before responding.

Under the GDPR, the time limit for responding to a subject access request is one month from the date of receipt. However, if a request is complex, the employer can extend the time period for response by a further two months.

## Notes

Where an organisation provides a form to assist with responding to subject access requests, it must still respond to requests that are made through other formats, such as email.

As the General Data Protection Regulation (GDPR) applies to all personal data that an organisation processes, employers should accept subject access requests received from workers, contractors, volunteers, interns and apprentices, as well as employees.

## Warning

Employers that fail to comply with their obligations under the General Data Protection Regulation (GDPR), including failing to comply with subject access rights, can be subject to significant administrative fines of up to €20 million or 4% of the undertaking's worldwide annual turnover, whichever is higher. Although the Information Commissioner will take into account a number of factors when determining the level of a fine, employers would be well advised to take subject access rights seriously in order to mitigate the risk of liability or enforcement action.

## Future developments

The General Data Protection Regulation (GDPR) will come into effect on 25 May 2018