Browne Jacobson

# New guidance for employers on subject access requests published by the ICO

26 June 2023

On 24 May 2023, the Information Commissioner's Office (ICO) published new guidance for employers and businesses on responding to subject access requests (SARs).

The guide is a helpful tool for organisations in ensuring they comply with their obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA) when responding to requests for personal data.

In particular, the ICO has supplemented the document with a useful 'SARs Q&A for employers page' which signposts some of the commonly arising issues for organisations, including those which have recently been the subject of sanctions.

Some of the key takeaways from the guidance and the new Q&A page are:

## 1. There are no formal requirements for a valid SAR

The guidance reminds organisations that SARs may be directed to any individual within an organisation; they may be made via social media; they do not need to include the words 'subject access requests'; and that they may mistakenly refer to legislation other than the UK GDPR and DPA but nevertheless constitute a valid SAR.

To safeguard organisations against the potential risk of failing to identify a SAR when submitted informally, the ICO encourages organisations to ensure all staff members are wary of the organisation's obligations to respond to SARs and can correctly identify them. Additionally, the guidance suggests that organisations employ designated individuals to respond to any SARs they may receive.

## 2. Strict time limits apply when responding to SARs

The guidance emphasises that a failure to comply with the time limits set on responding to SARs can result in regulatory action, including either financial sanctions or reprimands.

The ICO helpfully clarifies, however, that the time to respond to a SAR can be extended when the request is particularly complex, and that organisations have a right to seek clarification of the exact nature of the information sought by the requester before responding, thereby "stopping the clock" on the response time.

## 3. There is no obligation to respond if the request is manifestly unfounded or manifestly excessive

An organisation will also not be required to respond when disclosure would include, amongst other things, information identifying an individual other than the requester, a confidential reference, or documents subject to legal professional privilege. The guidance provides helpful examples of when these, and other exemptions, may be applicable and the recommended steps to adopt in determining their applicability.

## 4. Compliance with a SAR is required irrespective of whether the requester is in the process of the tribunal or

## grievance processes

However, if certain documents (such as witness statements) contain the personal data of third parties given in confidence then it may be inappropriate to disclose such documents. It's also important to note that whistle blowers are protected by the Public Interest Disclosure Act 1998.

## 5. Searches of all electronic systems are necessary

Personal information can include the contents of emails stored on computer systems and that disclosure may require providing redacted versions of email correspondence. A SAR may also require searches across social medical platforms, including Facebook, WhatsApp and Microsoft Teams chat channels to be conducted for any personal information shared about the requester.

## 6. Enforcement action may be taken due to non-compliance

According to the ICO, between April 2022 and March 2023, 15,848 complaints related to SARs were reported to the ICO. Where an organisation has failed to comply with a SAR, the ICO can take action by issuing a warning, reprimand, enforcement notice or penalty notice.

Non-compliance by way of delayed or non-response to a SAR has clearly been the most significant issue within the health and government sectors. For example, the ICO recently issued reprimands against both Norfolk County Council (Norfolk CC) and Plymouth City Council (Plymouth CC) for their statutory infringements relating to SARs. Investigations conducted by the ICO identified substantial delays on the parts of these councils in responding to SARs, with some requests still not have been responded to despite periods of up to two years passing since they were made. Notwithstanding the significant mitigating factors identified in each of these cases (which included, for example, the impact of the Covid-19 pandemic on the ability of Norfolk CC to access manual records, or the efforts of Plymouth CC to log and track SARs with KPIs), the ICO determined in both cases that reprimands were appropriate and made recommendations to both bodies to ensure their compliance with the GDPR and DPA.

While the guidance and new Q&A page have been published in the context of the ICO expressing its intention to move away from financial sanctions towards public reprimands, organisations should be reminded that reprimands can still act to significantly damage the reputation and should not be taken lightly.

Browne Jacobson's specialist data team is here to answer any questions you may have about your personal data obligations and guide you through your requirements when responding to a SAR.

# Contact


Mark Hickson

Head of Business Development

onlineteaminbox@brownejacobson.com

+44 (0)370 270 6000


## Related expertise

**Services**

Data protection and privacy | Freedom of information | Information law