

## Guide to information requests under the Data Protection Act

*For many organisations, a key problem with data protection legislation is handling requests for access to information. This guide outlines the key actions that an organisation should take when receiving a request for access to personal information.*

Under section 7 of the Data Protection Act 1998 (DPA), individuals are entitled to access the information that an organisation holds about them. This is an important right in data protection legislation, but can have a significant impact on businesses. Businesses must carry out detailed searches quickly within a deadline of 40 days from receipt of the request. The searching can expand to cover emails, databases, paper records and CCTV records. The maximum fee that may be charged to the individual (regardless of the breadth of the access request) is £10, with the cost of searching vastly exceeding this. Although there are some exceptions to the right of access, organisations are often concerned about the disclosure of prejudicial information.

### The request

#### What is an individual entitled to?

An individual is only entitled to information that relates to them (their ‘personal data’) that the data controller holds in electronic form or in a ‘relevant filing system’.

#### What is a ‘relevant filing system’?

The Information Commissioner’s guidance suggests that in most cases, paper records would amount to a relevant filing system for the purposes of the DPA if they are held in a ‘sufficiently systematic, structured way’. If the paper records are held in no particular order (i.e. unstructured), they may not be subject to the right of access.

#### Does the organisation process personal data?

The fact that an individual is named in a document does not mean that the entire document is the individual’s personal data. The leading case relating to access requests and personal data is *Durant*<sup>1</sup>. Durant

suggested that for information to be personal data it had to be “biographical in a significant sense” and that the individual making the request had to be the focus of the information. In *Durant*, information about the FSA’s enquiry into Mr Durant’s complaint against Barclays bank was not data personal to Mr Durant. This case has been followed by a number of cases in the First Tier Tribunal (Information Rights)).

#### What form does the subject access request have to take?

There is no prescribed format for a subject access request, provided that it is in writing. A written can be received by fax, email, post and even social media (e.g. to the organisation’s dedicated Facebook page or Twitter account). An organisation is not obliged to respond to a verbal request, unless it is satisfied of the person’s identity.

---

<sup>1</sup> *Michael John Durant v Financial Services Authority* [2003] EWCA Civ 1746

# What to do when a request is received

## 1. Ensure the request is logged and complied with promptly

Individuals do not have to say that they are making a subject access request or make reference to the DPA for it to be a valid request. Consequently, personnel who might receive such requests should be trained in data protection compliance so they can recognise a request for what it is and ensure it is dealt with promptly, within the statutory 40 day deadline. If an organisation does not comply with a request either promptly or fully, an individual can complain to the Information Commissioner who can take enforcement action.

## 2. Check that there is sufficient information to respond to the request

The organisation does not have to respond to a request until it has all of the information that it reasonably requires to respond and to be able to locate the information sought. The 40-day time limit for responding to the request will not start until this information, if requested, has been obtained. If the access request is not clear, the organisation is entitled to go back to the individual for more information.

Similarly, the time limit will not begin unless payment of the fee has been made (if the organisation is going to charge it).

## 3. Ensure that the individual making the request is entitled to the requested information

If the organisation is unsure of the identity of the requestor, it can ask them to provide evidence of their identity. Third parties, for example solicitors, can request data on someone else's behalf - although it is the responsibility of the third party to evidence their entitlement to represent the individual concerned. If an individual is writing on behalf of a spouse, or a legal representative on behalf of their client, an organisation should not assume that the requestor has authority to act on behalf of the client/individual. The organisation should ask for written evidence of authority. This could be through a written statement or a general power of attorney.

## 4. Carry out a search for the information requested

Once satisfied that it has enough information to carry out the search, the organisation should search for any relevant information which it may hold. Searches may encompass electronic documents (emails, database records etc.) and paper records (subject to the relevant filing system criteria, above).

Information held by a data processor on the controller's behalf will also be subject to an access request if it relates to the individual about whom an access request has been made.

Archived, but not deleted, data should also be searched.

## What exemptions may be relevant?

The DPA lists a number of exemptions to the obligation to disclose personal data. The most relevant of which are summarised below:

---

<sup>2</sup> [2007] All ER (D) 65

<sup>3</sup> [2012] Trago Mills (South Devon) Limited v The Information Commissioner, The First-Tier Tribunal, General Regulatory Chamber, Information Rights, Bristol. This case relates to Freedom of Information but the court's guidance in this case is more broadly applicable.

Exemption	Information (potentially) exempted
Confidential references	References given by the controller that are connected to actual or potential education, training or appointment of the data subject. This does not apply to references from a third party source.
Legal Privilege	Documents that are subject to legal professional privilege.
Management forecasts	Data used for an organisation's forecast or planning (to the extent that disclosure would prejudice the organisation's ability to conduct its business).
Negotiations with the individual	Information which relates to ongoing negotiations between the organisation and the individual requesting the information, where disclosure would prejudice those negotiations.
Prevention or detection of crime	Any information if its release would prejudice: <ul style="list-style-type: none"> <li>• the prevention or detection of crime;</li> <li>• the apprehension or prosecution of offenders; or</li> <li>• the assessment or collection of any tax or duty or of any imposition of a similar nature.</li> </ul>
Repeat requests	Identical or similar requests do not need responding to unless a reasonable time has elapsed or there is a reasonable circumstance.
Third Party Information	An organisation cannot refuse to provide access to personal data simply because the data refers to a third party source. Instead, the organisation is required to undertake a 'balancing act' to ensure the privacy rights of the individual requesting the data and the third party included in the data are respected. Where the data includes third party information, it may be possible to: <ul style="list-style-type: none"> <li>• anonymise the data relating to the third party;</li> <li>• seek consent from the third party; or</li> <li>• decide if the disclosure is reasonable, bearing in mind any duty of confidentiality owed to the third party as well as any statutory requirements.</li> </ul>

## The disclosure

The individual is entitled to a copy of their personal data, not a copy of the documents that contain their personal data.

The personal data disclosed needs to be provided in an 'intelligible form' - e.g. if codes have been used, a key to those codes should be provided so that the individual can understand the information. There is no requirement to make the data 'legible' or even understood by the recipient (e.g. translated into their native language).

## The response letter

In addition to enclosing a copy of the applicant's personal data (where this is being disclosed), the response letter should identify in general terms:

- What personal data have been processed;
- The sources of that personal data;
- The purposes for which their personal data is processed; and
- The recipients of that personal data.

## A note on automated decision-taking

Where an organisation makes decisions electronically without human intervention (e.g. automatic scoring after psychometric testing in graduate recruitment) ("automated decision taking"), an individual has the right to ask for information about that automated processing (trade-secret information is, however, exempt). Additionally the individual can ask that the decision is re-taken without the use of electronic means. The organisation has 21 days to respond to such a request.

An example of one of the limited exemptions from these obligations is where the automated decision-taking is undertaken for the performance of a contract (for example, the scanning of job applicants' CVs) or where required by statute.

If an individual does not ask for information about automated decision taking, the organisation is not obliged to provide it.

## Contacts



**Ruth Boardman**  
Partner  
ruth.boardman@twobirds.com  
Tel: +44 (0)20 7415 6018



**Laura Acreman**  
Associate  
laura.acreman@twobirds.com  
Tel: +44 (0)20 7905 6355

**twobirds.com**

**Abu Dhabi & Beijing & Bratislava & Brussels & Budapest & Copenhagen & Düsseldorf & Frankfurt & The Hague & Hamburg & Helsinki & Hong Kong & London & Lyon & Madrid & Milan & Munich & Paris & Prague & Rome & Shanghai & Singapore & Skanderborg & Stockholm & Warsaw**

Bird & Bird is an international legal practice comprising Bird & Bird LLP and its affiliated and associated businesses. Bird & Bird LLP is a limited liability partnership, registered in England and Wales with registered number OC340318 and is authorised and regulated by the Solicitors Regulation Authority. Its registered office and principal place of business is at 15 Fetter Lane, London EC4A 1JP. A list of members of Bird & Bird LLP and of any non-members who are designated as partners, and of their respective professional qualifications, is open to inspection at that address.