Freedom of Information: this time it's personal

Drawing on the significant relevant case law, Paul Gibbons aka FOIMan, gives practical guidance on applying section 40 FOIA (the personal data exemption)

Ostensibly, the Freedom of Information Act 2000 ('FOIA') gives everyone the right to access any information that they want. At the opposing end of the spectrum, we have the Data Protection Act 1998 ('DPA'), which exists to regulate the use of personal data. The personal data exemption at section 40 FOIA is designed to circumvent the apparent conflict between these two seemingly opposing aims. And according to central government statistics, section 40 is the most commonly used exemption. In applying it, practitioners must understand (and be able to apply) the DPA.

Those of us who are responsible for DPA and FOI compliance within our organisations are in a strong position to apply the exemption correctly. But FOI Officers who are not used to the DPA may well struggle with the complexities of the personal data rules.

To add to the complexity, data protection law is likely to change in the next three years with the introduction of a General Data Protection Regulation ('GDPR') across the European Union. If applying the exemption is challenging now, only more struggles await us in the coming years.

For the time being though, how should FOI Officers apply the section 40 exemption?

What is personal data?

FOIA uses the definition of personal data provided in DPA. Arguments abound over the interpretation of this definition but in summary, personal data have the following characteristics:

- they relate to an individual (therefore not a company) who can be identified from the data or other data in the possession of or likely to come into the possession of the organisation;
- the individual must be alive (information relating to the deceased is another matter entirely);
- the data must fall into one of five categories listed in the Act.

An amendment to the DPA made by FOIA introduced the fifth of the five categories, and its effect is that public authorities must interpret personal data more broadly than, for example, private businesses.

For FOI purposes, this is not necessarily a bad thing, as it has the effect of simplifying our understanding of what is personal data.

Only in borderline cases is it going to be appropriate to consider the definition at length. Practitioners will be relieved to know that a name, for example, is personal data (although they may be mystified that there was ever any doubt over this question).

FOI and subject access

The DPA gives individuals the right to access personal data about themselves held by organisations (or 'data controllers', in DPA-speak) by making what is called a 'subject access request' ('SAR'). Like FOI requests, SARs must be made in writing and need not cite the DPA.

If your organisation receives a written request from an individual for information relating to him or herself, it must be handled as an SAR under the DPA.

What if a requester states that they are making their request under FOI? Or if they make a request under FOI containing multiple questions, some of which would require the disclosure of personal information about them?

In such scenarios, the first subsection of section 40 is relevant and the requested data are exempt from FOIA. This, of course, does not mean that the requester cannot have their own information. It just means that the SARs provisions of the DPA is the appropriate route (just as environmental information is exempt from FOI but is available through the Environmental Information Regulations 2004). So the information relating to the requester should be dealt with under the DPA.

There are two options for how to proceed with dealing with such requests. The authority can issue a refusal to the requester citing the section 40(1) exemption, and requesting that they make a separate SAR. However, it is generally preferable to

(Continued on page 4)

(Continued from page 3)

answer the request without referring back to them.

The difficulty here is that there are different requirements for SARs and FOI responses.

SARS only have to be answered within 40 calendar days, and it is possible for organisations to charge a fee of £10. Proof of identity is also generally required.

Therefore whilst FOI Officers may not require the request to be resubmitted, they may well need to ask a requester to provide further information and payment, and explain that the personal information may be (legitimately) provided at a later date than other information they have asked for.

Third party personal data

When personal information relating to individuals other than the requester is captured by FOIA, the exemption at section 40(2) may be considered. It will apply if:

- disclosing the data would contravene one of the eight Data Protection Principles of the DPA;
- an individual affected has written to the public authority under section 10 of the DPA, requiring them not to provide data relating to them as it would cause them substantial damage or distress (and the public authority or a court has accepted this); and
- the individual(s) affected would not be entitled to the information if they made a SAR under the DPA due to a DPA exemption.

Under normal circumstances, it is the first of these that is relevant. But that is no cause for alarm; there is no need to scramble for your copy of the DPA just yet.

The only Principle that is relevant in the FOI context is the First Principle. This requires that personal data must only be used in a way that is fair and lawful. Not just that though; it must also meet at least one condition in Schedule 2 of the DPA, and if it is sensitive personal data (i.e. it relates to ethnicity, sexuality, politics, religion, trade union membership, health or criminal offences or proceedings), it must also meet a condition in Schedule 3 of the DPA.

All of this sounds rather complicated, doesn't it? Helpfully, there have been numerous decisions that clarify how it should be done. Another simplifying factor is that when we examine the two Schedules mentioned above, there are very few conditions that are relevant.

Approach to deciding whether to disclose personal data (from *Egan v IC & West Midlands Police*)

1. *Is the information personal data?*
2. *Is it sensitive personal data?*
3. *If the answer to the second question is 'yes', would disclosure fulfil at least one condition in each of Schedule 2 and 3 of the Data Protection Act?*
4. *If the answer to the third question is 'yes', would disclosure be otherwise fair and lawful?*

The Schedule 2 conditions

The two relevant conditions for FOIA purposes are 'consent' and 'legitimate interests'. In most circumstances, the latter will be the relevant consideration.

In *Goldsmith International Business School v the Information Commissioner and Home Office* (2014, UKUT 563 (AAC) 16th December 2014), the correct approach to deciding whether the condition applies was outlined. FOI Officers should ask themselves the following questions:

- is the data controller or the requester pursuing a legitimate interest;
- is the disclosure necessary to meet that interest; and
- will disclosure cause unwarranted prejudice to the rights and freedoms or legitimate interests of the individual.

The decision goes into considerable detail about how these questions should be interpreted. One significant point is that in order to demonstrate that disclosure is necessary, public authorities will need to consider if there would be other ways to achieve the legitimate interest without disclosing the information.

What is a legitimate interest in an FOIA context? For the most part, this will be the same as what is in the public interest (see *Innes v IC,* 13th February 2013, EA/2013/0044). However, this will not always be the case. Disclosures have been ordered where it is decided that a legitimate private interest will be met (see *Henderson v IC,* 26th February 2013 (EA/2013/0055)).

If the data are sensitive, FOI Officers will need to find another condition in Schedule 3 of the DPA to legitimise disclosure. Again, for practical purposes, there are only two likely options. The first is explicit consent — if the affected individual has actively indicated their agreement to the data being disclosed, perhaps in an email to the FOI Officer.

The other is where individuals have placed information in the public domain themselves. The fact that David Cameron is a member of the Conservative Party is sensitive personal data. We can write about it because he himself has told everybody that he is, not least when he stood for election as a representative of that party.

Clearly, it is much more difficult to justify the disclosure of sensitive personal data than ordinary personal data. It will be rare that such data will be disclosed through FOIA.

All the considerations, but not necessarily in the right order

So far, I have outlined a series of considerations that any practitioner will have to go through before deciding to disclose personal data. But how important is it to consider them in the same order each time?

With sensitive personal data, there is very little point in considering whether disclosure is fair and lawful if there is no condition that can be met.

In *Egan v IC & West Midlands Police* (28th November 2014, (EA/2014/0297)), it was suggested that the correct order should be:

- is the information personal data?;
- is it sensitive personal data?;
- if the answer to the second question is 'yes', would disclosure fulfil at least one condition in each of Schedule 2 and 3;
- if the answer to the third question is 'yes', would disclosure be otherwise fair and lawful?

Most practitioners would automatically jump to the last question before looking at the conditions, and the Information Commissioner has also taken this approach. However, the Information Tribunal has suggested that we should be less dogmatic.

In *Surrey Heath Borough Council v IC & Morley* (21st July 2014, UKUT 0330 (AAC)), Judge Jacobs said there was no distinction between the assessment of fairness and the process by which it is established whether the legitimate interests condition is met. He argued that 'the latter is but a specific instance of fairness.' This is another argument in favour of considering conditions first.

To disclose or not to disclose

In practice, FOI Officers will often have a gut instinct as to whether or not personal data ought to be disclosed.

The challenge is then to apply the process described above to ensure that whatever is decided can be confidently defended to the applicant, to those individuals affected and in addition to the Commissioner and anyone else who may be required to review the decision.

Following this approach will also act as a check on those gut instincts, and help prevent the inappropriate disclosure of personal data. With the Information Commissioner able to issue penalties of up to £500,000 for breaches of the Data Protection Principles, the consequences of getting it wrong can be significant. In this context, it is understandable why some practitioners may choose to play it safe when responding to requests which involve personal data.

Paul Gibbons
FOIMan
paul@foiman.com