How the GDPR affects the administration of FOIA

Paul Gibbons, aka FOIMan, explores the effect of the GDPR on FOI law and explains the major challenges for FOI Officers

The relationship between the Freedom of Information Act ('FOIA') and the Data Protection Act ('DPA') is one of the most difficult areas for practitioners to negotiate. In a previous article, I described the way that the two pieces of legislation work together ('Freedom of Information: this time it's personal', Volume 11 Issue 6, pp.3-6). Effectively, the various provisions of section 40 FOIA prevent the Act from conflicting with the DPA's obligations.

Readers will no doubt be aware that from 25th May 2018, a new data protection law will apply in the UK — the General Data Protection Regulation ('GDPR'). This means that section 40, along with the equivalent regulations in the Environmental Information Regulations 2004 ('EIRs'), will need to be amended to reflect the language and application of the new law.

However, this is not the only implication of the GDPR. Data controllers — organisations that determine how data will be used – should be considering how their existing use of personal data is affected by the new Regulation. Processing FOI requests involves the collection and storage of personal data about applicants and others. Practitioners therefore need to give thought to how GDPR affects the way that they handle FOIA requests.

In this article, I'm going to highlight the areas of FOIA administration to which practitioners will want to give most attention.

The Data Protection Bill and FOIA

Firstly let's look at the ways that FOIA itself will change as a result of the GDPR. As indicated above, the primary impact is on section 40 FOIA. The new Data Protection Bill ('the Bill'), first published in mid-September 2017, contains the relevant amendments in schedule 18. Before we examine the proposed changes, a note of caution: as with all Bills, there is the possibility that parts of the law will change before it is enacted. Therefore the following analysis is subject to any changes that might occur in the coming months.

As under the current arrangements, the most likely justification for refusing to provide personal data under FOIA is if disclosure would contravene the Data Protection Principles, now listed at Article 5 of the GDPR. The amendments apply the same condition to disclosure of 'manual unstructured data' (the equivalent of 'category (e) data' in the current DPA), which is not subject to the GDPR, but is covered by the 'applied GDPR' (a creation of the Bill).

The exemption – this time subject to a public interest test — will also apply to personal data where:

- an individual has objected to the disclosure of their information under Article 21 of the GDPR; or
- the data would be exempt from disclosure if the individual concerned made a subject access request under Article 15 of the GDPR or clause 43(1)(b) of the Bill (the latter providing for subject access to law enforcement data).

Section 40(5) FOIA is amended similarly in relation to the duty to confirm or deny whether personal data are held. Subsection (6) disappears altogether as it is no longer relevant. The definitions at section 40(7) are amended to remove references to the DPA and substitute equivalent references to the GDPR and the Bill.

In Volume 13 Issue 5 of this journal ('How will the GDPR affect FOI law?' pp.8-10), Curtis McClusky highlighted a problem that might have resulted in less information being disclosed under FOIA once the GDPR applies. Article 6(1)(f) of the GDPR indicates that public authorities cannot justify use of data by relying on the 'legitimate interests' condition. Currently, this is the usual legal basis for disclosures of personal data under FOIA. Thankfully, this is addressed by the new Bill which adds a new subsection (8) to section 40. The effect of this new provision is to remove the bar on public authorities using the legitimate interests condition when considering FOIA disclosures.

Similar amendments are made to the EIRs, and the Scottish versions of FOIA and the EIRs.

The GDPR

Broadly speaking, the requirements of the GDPR are very similar to the requirements of the DPA. The principles set out in schedule 1 of DPA survive for the most part at Article 5 of the GDPR. Unless exemptions apply, all processing of personal data must be in line with these principles, which are listed at figure 1. The conditions at Schedule 2 of the DPA, one of which must be met to legitimise the use of personal data, can now be found at Article 6 (see the list at figure 2).

Figure 1: the GDPR Article 5 Principles

(a) Lawfulness, fairness and transparency
(b) Purpose limitation
(c) Data minimisation
(d) Accuracy
(e) Storage limitation/ retention
(f) Integrity and confidentiality/security

5(2) Accountability

Figure 2: Lawful conditions set out at Article 6 of GDPR

(a) Consent
(b) Necessary for performance of a contract
(c) Necessary for compliance with a legal obligation
(d) Necessary to protect vital interests
(e) Necessary for performance of task in the public interest or in the exercise of official authority
(f) Necessary for the purposes of legitimate interests except where those interests are overridden by the interests or rights of the data subject.

Under the DPA, where data fell into the definition of 'sensitive personal data', a condition also had to be found at schedule 3 to justify their use. In the GDPR, we have instead 'special category data' which should be justified using a condition from a similar list at Article 9 of the Regulation.

One of the biggest differences in the GDPR is an increased emphasis on 'accountability'. Organisations including public authorities will need to be able to demonstrate what they are doing to ensure personal data are appropriately handled. Whilst it might have been acceptable in the past to 'fudge' DPA compliance, the intention of the GDPR seems to be to draw harder lines. What once was good practice will now be required behaviour. In terms of how we manage FOIA requirements, it will be necessary to identify the situations where personal data are collected, input, stored, shared, and otherwise processed, before considering how each of these uses can be justified under the GDPR.

One way in which accountability is demonstrated is through conducting 'Data Protection Impact Assessments' ('DPIAs'). Such assessments will be required for 'high risk' processing. Guidance from the Article 29 Working Party (the Committee made up of European data protection regulators, including the UK's Information Commissioner) suggests that processing will be 'high risk' where significant volumes of data are processed. Given the volume of requests made to some public authorities, consideration at least ought to be given to conducting such an assessment in relation to FOIA administration. If a DPIA were to be conducted, the following considerations would be relevant.

What personal data are processed by FOIA administrators?

The GDPR defines personal data as: 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person…'.

FOIA establishes that 'any person' can make a request. This will include 'legal persons' such as registered companies. The GDPR is very clear that it: 'does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person' (Recital 14).

Details of companies that make requests will not be covered by the GDPR. However, it is worth noting that sole traders and those in partnerships are 'natural persons'. Therefore it cannot be assumed that data protection rules are irrelevant whenever a request is received from a business – it will depend on the status of that business. Practitioners should also be cautious in handling data about the employees of a company, such as the name of the employee that makes the request on their employer's behalf.

If a request is made by a 'natural person', what information will be covered by the GDPR? Section 8 FOIA requires that applicants provide their name and an address for correspondence, together with a description of the information that they require. Names and addresses, particularly together, are likely to ensure that the person can be identified. Put together with the name and address of the applicant, the information asked for will also be personal data. As far back as 2003, the Durant case (*Durant v Financial Services Authority* [2003] EWCA Civ 1746) established that one of the tests of personal data, even under the present law, is whether the data are 'biographical in a significant sense'. What a person might be interested in and how they ask for it

(Continued on page 6)

(Continued from page 5)

when they make a FOIA request can tell us a lot about them.

Even if the information requested is separated from the name and address of the applicant, it is perfectly feasible for it to be personal data. The test is whether the individual can be identified. A request about roadworks outside a specific address, examination criteria for a university course with only a small number of students enrolled, or information relating to a dispute involving two individuals, may all be specific enough for colleagues or others to identify the applicant even if their name is withheld. Handwriting or the idiosyncratic expression of a request could similarly be used to identify an individual.

This is all information that is supplied by the applicant. In addition though, public authorities may create and retain other information about applicants. It is common practice to categorise applicants – are they 'ordinary' members of the public, businesses, campaigners, or journalists? Based on this, the press office might be alerted about a request. The result is that additional data are added to FOIA records systems describing the nature of the applicant.

Some authorities may go further and seek to discover whether the applicant has made the same request to other authorities. In doing so, they are collecting and sharing more personal information about them.

Additionally, employees involved in processing an FOI request may unwisely record their opinions of the applicant. This will also be the applicant's personal data.

Depending on local procedures and specific circumstances, there might be other details recorded about an applicant that would constitute their personal data. Whenever such data are recorded, public authorities will need to ensure that they comply with the GDPR.

How can authorities demonstrate compliance with the GDPR?

Authorities will need to comply with the principles listed at Article 5 (see figure 1) and with other responsibilities set out in the GDPR when processing data about applicants and their requests. In order to meet the accountability principle at Article 5 (2), they will need to evidence this compliance.

A privacy notice containing the required elements listed at Article 13 of the GDPR will provide evidence that an authority is attempting to meet principle (a) in that it is handling data fairly, lawfully and transparently. It will be appropriate to demonstrate that consideration has been given to how to make this information as accessible as possible to applicants, given that they may not all visit the authority's website before making a request. The notice will need to identify which legal basis of those identified at Article 6 justifies the processing of applicants' personal data (see figure 2). For the most part, it is likely that 'processing is necessary for compliance with a legal obligation to which the controller is subject'. However, this will not justify all processing of applicant data. The obligation to respond to FOIA requests is unlikely in all cases to require, for example:

- sharing the identity of applicants in an uncontrolled way across the authority;
- categorising applicants (e.g. journalist, campaigner, private individual, etc);
- 'flagging' particular applicants for special treatment (e.g. notifying press officers that a request has been received from a journalist);
- 'Googling' applicants; or
- discussing 'round-robin' requests with other practitioners or authorities.

It is certainly possible to justify doing any or all of the above in a particular case, but practitioners will need to give thought to which of the legal justifications at Article 6 will apply.

Processing applicant data for reasons other than answering a request may also breach principle (b), unless applicants have been warned in advance about the various ways that their data may be used. The preparation of monitoring statistics on FOIA compliance will not be such a breach, since Article 5 makes it clear that such a use of data will be compatible with any original purpose.

Practitioners will also need to ensure that their FOIA procedures address how the collection of applicant data is kept to a minimum (principle c), how data will be kept as accurate as necessary for the processing of requests (principle d), and how long they will be retained in an identifiable form (principle e). Many authorities delete information about the applicant from their systems after a specified period, retaining only details of the request itself. Such an approach would be consistent with this last principle. It would be wise to ensure that this policy is documented in the authority's retention schedule.

The last of the principles at Article 5(1) is equivalent to the Seventh Principle in the DPA and requires organisations to keep personal data secure and to protect them against unauthorised or unlawful use or accidental loss, destruction or damage (principle f). Naturally it is important to take appropriate precautions (or 'technical or organisational measures') to ensure that records of applicants are secured. The duty to protect personal data is further reinforced by Article 32 of the GDPR. Practitioners will want to review the security of systems used to manage FOIA requests, but also their vetting processes for responses (bearing in mind high profile accidental disclosures in the past). They should ensure that they have documented any risks identified and improvements made.

I referred above to the 'uncontrolled' sharing of applicant data across authorities. One method of securing data promoted by the GDPR is the use of 'pseudonymisation'. This is defined in the GDPR as: 'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific

data subject without the use of additional information, provided that such additional information is kept separately…'.

Removing the names of applicants before circulating requests internally could be described as a form of pseudonymisation, thereby reducing the risk of applicants' personal data being lost. It can also serve to limit the possibility of applicant data being used in an unfair or incompatible manner (e.g. handling their request differently on account of their identity).

Rights of data subjects

The GDPR provides for a number of rights for data subjects. Many of these are very similar to the rights they currently have under the DPA. For example, individuals will be able to make subject access requests which might (for example) reveal how their FOIA request was handled. It would be worthwhile reminding colleagues that anything they write down about the applicant or their request may have to be disclosed.

Applicants will also be able to object to use of their data on public interest grounds, and to seek the erasure of data that are no longer required. These rights are not absolute, but practitioners will need to consider how they would meet these requests should this be required.

The GDPR requires that applicants are regularly reminded of their rights, which might be demonstrated by incorporating a standard clause in FOIA response templates.

Overseas transfers

Like the Eighth Principle of the current DPA, Chapter V of the GDPR requires that certain conditions are met before transferring data overseas. Whilst for the most part, this is unlikely to be a major factor affecting the processing of FOIA requests, practitioners will need to demonstrate that they have considered this.

For example, a public authority might process FOIA requests in the 'cloud'. They would need to ensure that the contract with the cloud service provider specifies either that the data must be stored within the European Economic Area ('EEA'), or provides some means of meeting the GDPR's requirements for processing overseas, such as incorporating a standard data protection clause adopted by the European Commission.

Controllers and processors

It is becoming increasingly common for public authorities to share the provision of services, including in some cases, the handling of FOIA requests. It will be essential in these circumstances for responsibilities to be clear and documented.

Practitioners will need to be able to demonstrate that they understand the nature of the relationship between the authorities. For example, whether they act as 'joint controllers' or whether one authority acts as a 'processor'. Where the latter applies, it will be necessary to ensure that a contract is in place, and the other authorities involved will need to show that data protection compliance is regularly audited.

Conclusion

In this article I have sought to draw attention to the range of activities involved in handling FOIA requests that require the processing of personal data. The DPA already imposes restrictions on the way that such personal data can be used.

With a new law on the way, the opportunity presents itself to re-examine these processes and ensure that they are consistent with the GDPR. In particular, practitioners will want to consider the following:

- what, and how, are applicants told about how their personal data will be used in the handling of their request;
- is it possible to identify a legal basis for every use of applicant data;
- what precautions are in place to ensure that the bare minimum of data are recorded and shared about applicants, that data are kept no longer than necessary, and that they are kept securely;
- is everyone aware of the implications of the GDPR for their work, and for the handling of FOIA requests; and
- how it can be evidenced that these issues have been considered and addressed.

For information on the training course 'FOI and Data Protection —How they Work Together', see www.pdptraining.com

Paul Gibbons
FOI Man
paul@foiman.com