How will the GDPR affect FOI law?

Curtis McCluskey, Associate with Reed Smith, assesses the impact on FOIA of incoming changes to the data protection landscape

The Freedom of Information Act 2000 ('FOIA') will be affected by the European General Data Protection Regulation ('GDPR'), which is due to come into effect on 25th May 2018. This position stands even after the event of Brexit, as the UK government has repeatedly confirmed its intentions for new UK data protection legislation to track the requirements of the GDPR.

The main impact on FOIA is to section 40, which interlinks the Act with the Data Protection Act 1998 ('DPA') — the law that the GDPR will replace. There is also a secondary impact: that organisations including public authorities will be obliged under the GDPR to document their compliance, meaning public authorities who also have duties to be transparent to the public will have no place to hide.

This article examines these two issues. First, with regard to the primary issue, a brief look at how the current law operates.

Current position

Looking closely at section 40 FOIA, the exemption regarding personal data accounts for two possibilities:

- an individual has made an FOI request for their own personal data, which should therefore be treated as a subject access request under the DPA (section 40(1) FOIA); or
- responding to the FOIA request would reveal third party personal data, and to release this information would breach the principles of the DPA (section 40(2) FOIA) — therefore requiring a consideration of whether there would be such a breach in the event of disclosure.

The first sort of FOI request is likely to be unaffected by the incoming GDPR, although public authorities will need to familiarise themselves with and make reference to the new GDPR provisions which deal with subject access requests.

However, dealing with the second type of request—where other people's data are involved — has become more uncertain. Largely, that is because assessing whether Data Protection Principles of the DPA will be breached is now a matter for EU interpretation rather than UK common law/precedent.

For the purposes of disclosure under FOIA, it is usually only the First Data Protection Principle (that personal data shall be processed fairly and lawfully and, in particular, must benefit from one or more specific conditions) that is relevant. As seasoned FOI practitioners are already aware, this requires FOI Officers to address the data protection rights of individuals, and to balance those rights against the legitimate interests in processing personal data. So how will this change under the GDPR?

GDPR takeover

Given the explicit reference to the DPA in FOIA, it will have to be amended to reflect the new GDPR. For this reason, interpretations around the section 40 exemption, drawn from the current data protection framework, are likely to change.

After 25th May 2018, the Information Commissioner's Office ('ICO'), Tribunal and courts will be required to interpret section 40 in light of the GDPR. Although they may look to previous rulings given that many of the DPA's underlying principles remain unchanged in the GDPR, previous rulings are no longer 'failsafe' and it will very much be a shifting landscape.

Currently, when dealing with section 40(2) FOIA cases, in determining whether it is fair and lawful to disclose information containing personal data via FOIA, public authorities consult Schedule 2 of the DPA to consider what grounds to rely on. In practice, 'legitimate interests' is usually the relevant ground.

Schedule 2 of the DPA is now being replaced with Article 6 of the GDPR — 'lawfulness of processing' — which continues to include 'legitimate interests' as a ground for lawful processing. However, the GDPR restricts the application of Article 6(1)(f) preventing its use by public authorities 'in the performance of their tasks.'

This provision alarmed the ICO, which in an analysis paper on the Proposed new EU General Data Protection Regu-

lation in February 2013 commented:

"We are unclear as to how Article 6 can act as gateway for legitimate processing triggered by Access to Information or Freedom of Information laws. In the UK, the trigger on Schedule 2 condition 6 currently offers this gateway. We would urge consideration of an explicit article recognising the interaction with FOI/Access laws."

Despite the ICO's concerns, the restriction made it through to the final text. Recital 47 offers an explanation as to why public authorities' reliance on Article 6(1)(f) has been removed. It provides:

'Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks.'

With the gateway removed, it is difficult to see how public authorities can justify disclosure of personal data without contravening the Data Protection Principles. It would seem that the only other possible ground public authorities may rely on is that the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority (Article 6(1)(e)). Indeed, Recital 45 to the GDPR indicates that Article 6(1)(e) could apply to public authorities. For instance, it provides:

'It should…be for Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law.'

It is difficult to say definitively whether this will be the route which public authorities will rely on after the GDPR takes effect. In any event, it seems like a very different analysis will be required of public authorities applying section 40(2). If Article 6(1)(e) is to apply to public authorities, it will likely fall to the UK government to determine the interplay with FOIA and other laws regarding access to information.

> ***"There will be no hiding. Public authorities' GDPR compliance efforts are as good as in the public domain, which will mean wider scrutiny and possibly also reputational impact should compliance efforts fall short in any way."***

Effect of GDPR's accountability and documentation requirements

Turning now to the second issue: the GDPR is heavier on accountability than is the Data Protection Directive (95/46/EC). This of itself is important for public authorities to pay attention to alongside their duty to be accountable (in a more general sense) to the public.

FOIA's key objective is to allow any member of the public to request access to any recorded information held by a public authority. Any document held by a public authority is disclosable under FOIA unless an exemption applies: this includes any documents an organisation holds regarding its data protection compliance.

If a requester asks for information on a public authority's data protection practices, responding to FOIA requests of this nature could be problematic if disclosing the documents reveals compliance failings under the GDPR, or even worse, reveals that no data protection compliance measures have been adopted, particularly where there are no documents to disclose.

There will be no hiding. Public authorities' GDPR compliance efforts are as good as in the public domain, which will mean wider scrutiny and possibly also reputational impact should compliance efforts fall short in any way.

One example of the new accountability requirements is in Article 30 of the GDPR, which requires organisations to maintain records of processing activities. Each controller is required to record the following information:

- name and contact details of controller, controller's representative, and the Data Protection Officer;
- a description of the purposes behind the processing of personal data;
- a description of categories of data subjects and categories of personal data;
- categories of recipients to whom personal data will be disclosed – including recipients in third countries or international organisations and, where applicable, the identity of the third country/ international organisation;
- the envisaged time limits for erasure of the different categories of data; and
- a description of the technical and organisational security measures in place to safeguard personal data.

It is open to requesters of information to ask for a copy of such a record. Unless there is a good reason to not disclose this information, public authorities will be required to reveal it.

Not only is it a requirement to maintain a record of processing activities, it is important that the details of the processing are accurately reflected in that document and are compliant with data protection laws. For example, the description of purposes for processing personal data in the documented record must be accurately reflected in the public authority's privacy policy. If it is not, the public authority could be criticised for not being open and transparent with how it is processing personal data.

(Continued on page 10)

(Continued from page 9)

In addition, organisations are required to document any personal data breaches (Article 33(5) GDPR), which include the facts relating to the breach, its effects and any remedial action taken. For public authorities, this document will become 'recorded information' and is therefore disclosable under FOIA. Revealing a documented record of data breaches could lead to wider scrutiny of data protection failings if the record shows there have been numerous breaches.

Currently, although it is considered best practice to document all data breaches, there is no strict legal requirement to do so. If no document exists, it may be difficult for a requester to obtain the information without triggering the costs exemption (complying with the request would exceed the appropriate limit prescribed under section 12 FOIA: 18 hours of resource). However, in light of the new rules around documenting breaches, the current possibility for public authorities to confirm in response to an FOI request that no document recording data breaches is available, will no longer exist come May 2018.

Conclusion

Following May 2018, it seems that public authorities may face some initial challenges with the application of section 40(2) exemption, if the request for information contains personal data belonging to a third party. The 'legitimate interests' ground commonly relied upon by public authorities to justify disclosure of personal data will be gone. Consequently, it may prove difficult for public authorities to ever disclose personal data through FOIA.

Furthermore, given the main objective behind FOIA — to increase accountability of public authorities, making their internal practices and decision-making disclosable to the world at large — there will be no way for public authorities to conceal any half-hearted GDPR compliance efforts. This accountability now extends to GDPR compliance, which itself explicitly requires for particular records to be in place, and which will qualify as 'recorded information'. For public authorities subject to FOIA, there is now no escape from data protection compliance.

Curtis McCluskey
Reed Smith
cmccluskey@reedsmith.com