The Subject Access under GDPR

When the General Data Protection Regulation (GDPR) comes into force on 25th May 2018, it will introduce a number of new obligations on Data Controllers which will require them, amongst other things, to review their approach to personal data breaches, privacy notices and overall GDPR compliance responsibility. Some new Data Subject rights, including the right to erasure and the right to data portability, will also be introduced.

So there is a lot to learn and do within a short space of time. The good news though is that, whilst GDPR will replace the UK's Data Protection Act 1998 (DPA), it still includes familiar concepts such the right of the Data Subject to request a copy of his/her data, known as a Subject Access Request (SAR) in DPA parlance.

In brief Article 15 of GDPR gives an individual the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information

The supplementary information mentioned above is the same as under section 7 of the DPA (e.g. information about the source and recipients of the data) but now also includes, amongst other things, details of international transfers, other Data Subject rights, the right to lodge a complaint with the ICO and the envisaged retention period for the data.

Fees

Under the DPA, Data Controllers can charge £10 for a SAR (£50 for a health record). GDPR allows most requests to be made free of charge. This is a significant change and will hit the budgets of those who receive voluminous or complex requests e.g. local authority social services departments. However, a "reasonable fee" can be charged for further copies of the

same information and when a request is manifestly unfounded or excessive, particularly if it is repetitive. The fee must be based on the administrative cost of providing the information.

Time Limit

The DPA allows Data Controllers 40 calendar days to respond to a SAR. Under GDPR the requested information must be provided without delay and at the latest within one month of receipt. This can be extended by a further two months where the request is complex or where there are numerous requests. If this is the case, the Data Subject must be contacted within one month of the receipt of the request and explain why the extension is necessary. All refusals must be in writing setting out the reasons and the right of the Data Subject to complain to the ICO and to seek a judicial remedy.

Format of Responses

Where the Data Subject makes a SAR by electronic means, and unless otherwise requested by the Data Subject, the information should be provided in a commonly used electronic format. Before providing the information, the Data Controller must verify the identity of the person making the request using "reasonable means".

The GDPR (Recital 63) introduces a new best practice recommendation that, where possible, organisations should be able to provide remote access to a secure self-service system which would provide the individual with direct access to his or her information This will not be appropriate for all organisations, but there are some sectors where this may work well e.g. local authorities may look to providing secure online access to social work records.

Article 15 makes it clear that the right to obtain a copy of information or to access personal data through a remotely accessed secure system should not adversely affect the rights and freedoms of others. Therefore, as is the case under section 7(4) of the DPA, careful thought will need to be given to whether third party personal data needs to be redacted before disclosing information.

Exemptions

Data Protection Officers will be familiar with the exemptions in the DPA, set out in Part 4 and Schedule 7, some of which allow a Data Controller to refuse a SAR. There is currently no such list in the GDPR. However Article 23 allows national governments to introduce exemptions to various provisions in GDPR, including SARs, by way of national legislation based on a list set out in that article. This contains the same categories as in the DPA e.g. national security, crime prevention, regulatory functions etc. My guess is that the UK Government will enact the same exemptions as currently exist in the DPA.

Recital 63 states the purpose of the SAR is to make Data Subjects aware of and allow them to verify the lawfulness of the processing of their personal data. This seems to suggest that requests for other purposes e.g. to assist in litigation may be rejected. Compare this to the recent case of Dawson-Damer v Tayor Wessing LLP [2017] EWCA Civ 74 in which the Court of Appeal said that there was nothing in the EU Data Protection Directive (which the DPA implements into UK law) which "limits the purpose for which a data subject may request his data, or provides data controllers with the option of not providing data based solely on the requestor's purpose." (More on this case here.)

The GDPR does not introduce an exemption for requests that relate to large amounts of data, but a Data Controller may be able to consider whether the request is manifestly unfounded or excessive. Recital 63 also permits asking the individual to specify the information the request relates to.

Subject Access and Data Portability

How different is the Subject Access Right to the Right to Data Portability set out in Article 20? The latter also allows for Data Subjects to receive their personal data in a structured, commonly used and machine-readable format. In addition it allows them to request it to be transmitted to another Data Controller.

Unlike the subject access right, the Data Portability right does not apply to all personal data held by the Data Controller concerning the Data Subject. Firstly it has to be automated data. Paper files are not included. Secondly the personal data has to be knowingly and actively provided by the Data Subject. By contrast personal data that are derived or inferred from the data provided by the Data Subject, such as a user profile created by analysis of raw smart metering data or a website search history, are excluded from the scope of the right to Data Portability, since they are not provided by the Data Subject, but created by the Data Controller. Thirdly the personal data has to be processed by the Data Controller with the Data Subject's consent or pursuant to a contract with him/her.

In contrast, the subject access right applies to all personal data about a Data Subject processed by the Data Controller, regardless of the format it is held in, the justification for processing or its origin.

It is important to not that both rights do not require Data Controllers to keep personal data for longer than specified in their retention schedules or privacy polices. Nor is there a requirement to start storing data just to comply with a request if received.