Data subject access requests: two opinions on the scope of the right

Two new opinions concerning the scope of data subject access requests under the GDPR have been handed down by advisors to the judges of the European Court of Justice (known as Advocate Generals). We round up the headline points and consider the implications for employers.

Is a data subject entitled to know the identity of employees of the data controller who have accessed their personal data?

In the first case, the data subject worked for, and was also a customer of, a bank based in Finland. He made a data subject access request and argued that he was entitled to know the names and job roles of all the people within the organisation who had viewed his personal data (both in his capacity as an employee and as a customer). The bank refused to provide this information, arguing that the right of access enshrined in the GDPR did not extend to log data of the Bank's processing system, which recorded which employees had accessed the system and when.

In the Advocate General's opinion, the right of access within the GDPR does not give a data subject the right to know the identity of employees who have accessed their personal data, where such employees were acting on the instructions of the data controller. Nor could employees acting under the bank's instructions be regarded as "recipients" of personal data. This is an important point since data subjects are entitled to

know the recipients or categories of recipients of their personal data.

You can read the Advocate General's opinion **here**.

Is a data subject entitled to receive a copy of the documents containing their personal data?

In the second case, the European Court of Justice (ECJ) was asked to rule on the right of a data subject to receive a copy of their personal data. The Advocate General opined that a data subject's right to a "copy" of their personal data means a right to be given a faithful reproduction of the data in intelligible form. The exact format of the copy is to be determined by: (i) the specific circumstances of each case; (ii) the type of data requested; and (iii) the needs of the data subject. Although there is no automatic right to obtain a partial or full copy of the documents containing the personal data, this may need to be provided where it is necessary to ensure that the personal data is fully intelligible. An example of this might be personal data contained in messaging platforms commonly used in the workplace such as Slack, where a basic export of the data is unlikely to be viewed as intelligible.

You can read the Advocate General's opinion **here**.

What does this mean for employers?

It is important to pause to note that neither of these opinions are strictly binding on the UK Courts. Nor are

Advocate General opinions even binding on the ECJ – although they are influential and tend to be followed. The ECJ decisions in these two cases are expected shortly. ECJ decisions are also not binding in the UK, however, they may be taken into consideration by the UK Courts and the UK data protection regulator (the Information Commissioner's Office (ICO)) where relevant to a matter before them. Given that UK data protection law is based upon the GDPR, it is likely that a UK Court and/or the ICO would have regard to relevant ECJ decisions. Furthermore, ECJ decisions concerning data protection remain relevant to employers with operations in member states of the EU, where the GDPR applies.

In the meantime, the first opinion will strengthen an employer's ability to resist requests for disclosure of the identity of employees who have accessed an individual's personal data. The second opinion simply underlines and reinforces the existing position in the UK, as set out in the **ICO's guidance** on data subject access requests and reflected in previous decisions of UK courts. The ICO guidance provides that:

"**the right of access enables individuals to obtain their personal data rather than giving them a right to see copies of documents** containing their personal data. You may therefore provide the information in the form of transcripts of relevant documents (or of sections of documents that contain the personal data), or by providing a print-out of the relevant information from your computer systems. While it is reasonable to supply a transcript if it exists, we do not expect controllers to create new information to respond to a SAR. Although the **easiest way to provide the relevant information is often to supply copies of original documents, you are not obliged to do so**." (emphasis added)

Brahams Dutt Badrick French LLP are a leading specialist employment law firm based at Bank in the City. If you would like to discuss any issues relating to the content of this article, please contact Amanda Steadman (AmandaSteadman@bdbf.co.uk) or your usual BDBF contact.