Bird & Bird

UK Information Commissioner offers advice to the UK finance sector on how to improve data subject access right processes following increase in complaints

01 October 2024

Following on from our last Fintech Features article in which we flagged that the European Data Protection Board (the committee of all the national data protection authorities in the EU) had chosen **data subject access rights** as a topic for "coordinated enforcement action" in 2024, the UK Information Commissioner's Office ("**ICO**") recently singled out compliance with data subject access requests ("**DSARs**") in the finance sector. In a LinkedIn post in August 2024, the ICO notes that the finance sector has recently seen a 15% increase in DSAR-related complaints and provides some pointers for organisations on how to improve. The ICO recommends the use of its Accountability Framework. Accountability is one of the key principles under UK GDPR - it requires organisations not only to comply with the law but *to be able to demonstrate their compliance with the law*.

The ICO suggests that organisations in the finance sector take three steps to improve compliance:

1. Assess your current compliance. The ICO advises organisations to look at their DSAR procedures and training to ensure that they are delivering compliance. The ICO's Accountability Framework has a list of questions to help organisations assess whether their approach is UK GDPR-compliant and work out where improvements may be required. For example:

Informing individuals and identifying requests:

- Would individuals say that you provide useful materials to help them to exercise their rights?
- Do your policies and procedures set out processes for dealing with DSARs?
- Do all your staff receive training and guidance about how to recognise DSARs and where to send them?

Monitoring and evaluating performance:

- Does your organisation monitor how your staff handle DSARs and use that information to make improvements?
- Does your organisation produce regular case assessments/reports to ensure that DSARs are handled appropriately, which are then shared with senior management who take appropriate action?
- Does your organisation analyse any trends in the nature or cause of DSARs to improve performance or reduce volumes?

Resources:

- Do you have specific staff responsible for managing DSARs, which ensures that they are appropriately handled even in case of staff absences?
- Do those staff receive specialised DSAR training, including regular refresher training?
- Would those staff say that your organisation has appropriate and sufficient resources to deal with the volume of DSARs even with a spike in the number of DSARs or reduction in staffing levels?

Logging and tracking requests:

- Does your organisation log receipt of all verbal and written DSARs and update the log appropriately (including the due date, any disclosed or withheld information, the actual date of the final response and action taken)?
- Do you have a checklist recording the key stages in each DSAR process/case e.g. which systems have been searched (either as part of the log or separately)?

Handling complaints:

- Do you have procedures in place to handle DSAR-related complaints raised by individuals and do you report their resolution to senior management?

2. Think about records management. The ICO says that if you know what information your organisation holds about people, where you hold it and how you can search for it, it will be much easier to handle DSARs.

The ICO advocates having:

- a well-structured file plan;
- standard file-naming conventions for electronic documents (to make them easier to search in response to a DSAR); and
- a clear retention policy detailing when to keep and delete documents.

Refer to the ICO's advice on locating information in response to a DSAR and also assess your approach against the ICO's Accountability Framework. For example:

Creating, locating and retrieving records:

- Do you have policies and procedures in place to ensure that you appropriately classify, title and index new records in a way that facilitates management, retrieval and disposal?
- Have your staff been trained to do this appropriately?
- Does your organisation identify the manual and electronic record-keeping systems which it uses and have an up-to-date information asset register?
- Has your organisation experienced any issues locating records?

Retention schedule:

- Do you have a retention schedule based on business need with reference to statutory requirements and other principles?

- Does that schedule provide sufficient detail to identify all records and to implement disposal decisions in line with the schedule?
- Are staff aware of the retention schedule and do they adhere to it in practice?
- Do you regularly review retained data to identify opportunities for minimisation, pseudonymisation or anonymisation and do you document this in the schedule?

3. Consider your organisation's culture. The ICO stresses that good information management and DSAR compliance rely on the entire organisation – not just the data/information management team or the data protection officer. Does everyone in your organisation understand the role they have to play so that there is an embedded culture of data protection compliance? Or does your organisation still procure systems which store personal data which are not easily searchable within the tight statutory deadlines for complying with DSARs? Data protection training and awareness throughout your entire organisation are key here. Again, the ICO's Accountability Framework has a list of suggestions to help you assess and, if necessary, remediate this.