"Knock knock… It's the ICO!"

The UK regulator's powers of entry and inspection

July 2018

This article first appeared in the Privacy Laws & Business UK Report, Issue 98 (July 2018).

The Data Protection Act 2018 ("DPA 2018") sets out the UK Information Commissioner's Office ("ICO") powers to enter and inspect business premises. These expanded powers are similar to those already held by UK and EU antitrust authorities, which are commonly referred to as 'dawn raid' powers. Failing to cooperate with, or to provide relevant information to, the ICO during such inspections can have serious consequences for both individuals and businesses. It is therefore important that businesses prepare for the possibility of on-notice and unannounced inspections by the ICO as this will reduce the immediate disruption and longer term legal and business risks.

Background

The Facebook/Cambridge Analytica investigation by the ICO in March this year highlighted some of the deficiencies in the ICO's array of enforcement powers under the previous regime. The DPA 2018 was not yet in final form at the time so the ICO's powers were more limited. However, the media and political storm around Cambridge Analytica combined with the challenges the ICO experienced in getting access to relevant premises (and data sources) were catalysts to the enhancement of the ICO's enforcement powers in the final version of the DPA 2018.

The ICO's enforcement powers

The DPA 2018 provides for a variety of inspections and other powers for the ICO, including:

- the power to request, by written notice, certain information from a controller or processor. In urgent cases, the ICO can request the specified information within 24 hours of the notice;
- the right to apply to the court for an order where a person has failed to comply with an information notice;
- the power to issue assessment notices to check whether a controller or processor is complying with the data protection legislation. This includes the right to carry out on-notice inspections of premises and equipment and, in some cases, to enter and inspect premises with minimal or even no notice; and
- the power to issue enforcement notices in respect of breaches of the GDPR/DPA 2018. In urgent cases the ICO can request that the requirement (to take action or to refrain from taking certain actions, or both) is complied with within 24 hours.

Some of the above powers will be familiar as they were included in the Data Protection Act 1998 ("DPA 1998"). However, the ICO can now require compliance within much tighter timeframes and obtain the support of the court where necessary.

Wider scope for compulsory inspections

The ICO's powers to issue assessment notices are broader in scope than those under the DPA 1998, under which the ICO could only target UK government departments and NHS bodies. Under the DPA 2018, any private sector UK business that controls or processes personal data can now be subject to compulsory inspections. This reflects the position in the GDPR which grants regulators the power to obtain access to controllers' and processors' premises, equipment and data in accordance with Member State procedural law. What the ICO can require in an assessment notice under the DPA 2018 has not changed substantially from the public sector assessment notice procedure in the DPA 1998.

When can the ICO enter and inspect premises with little or no notice?

Where the ICO has reasonable grounds for suspecting a data controller or processor of breaching the GDPR/DPA 2018 it can effectively accelerate the assessment notice process or inspect premises with no notice (where it is looking for evidence of breaches of the GDPR/DPA 2018 or evidence that offences under the DPA 2018 have been committed).

In particular, if the ICO believes it is necessary for a controller or processor to comply with an assessment notice requirement within less than 7 days, the notice period provided can be minimal or even potentially non-existent. In practice, this means that some of the protections relating to the assessment notice process (e.g. the right to appeal) will be unavailable or significantly less effective during an inspection on minimal or no-notice.

However, the above powers are subject to some important limitations, including the requirement to obtain a warrant in the following cases.

Obtaining warrant for non-compliance/offences

If the ICO wishes to enter and inspect premises to find evidence of non-compliance (or evidence that offences have been committed) under data protection legislation, it must apply to a judge for a warrant. The judge must be satisfied that there are reasonable grounds for suspecting: (i) a breach of specified provisions of GDPR/DPA 2018, or that an offence under the DPA 2018 is being committed; and (ii) that evidence of the breach or an offence is to be found on the relevant business premises. Such a warrant will permit the ICO to enter and search business premises and inspect equipment used for or intended to be used for processing personal data.

Obtaining a warrant in relation to an assessment notice

Where the ICO has issued an assessment notice that has not been complied with, it can apply for a warrant to enable it to enter and inspect premises to assess compliance. In this case, the judge only has to be satisfied that a controller or processor has failed to comply with a requirement in that notice.

Further thresholds for warrants

In both of the above cases, where the ICO is seeking to enter and inspect premises with minimal or no notice, the judge must also be satisfied either that giving (further) notice of a demand to access business premises would defeat the object of the inspection in the first place or that the Commissioner requires access to the premises urgently. In practice, a likely argument to satisfy either of those conditions is that the business in question would destroy evidence before the ICO could exercise its other powers. It is worth noting that the contents of a warrant will grant the ICO stronger powers than those under an assessment notice. For instance, under a warrant the ICO will be permitted to search premises, seize documents and require individuals on the premises to provide information.

At a reasonable hour

The ICO's powers to enter and inspect premises with little or no notice can only be exercised at a 'reasonable hour' (likely to be business hours) within seven days of the warrant being issued, unless the ICO considers that undertaking an inspection at such an hour would defeat the purpose of the inspection (e.g. because it would allow the business to destroy evidence before the ICO could exercise these powers).

Legally privileged information

The ICO cannot require the production of information which is legally privileged, specifically in respect of communications between a professional legal adviser and that adviser's client that: (i) comprise legal advice with respect to data protection legislation (legal advice privilege); or (ii) relate to proceedings under or arising out of data protection legislation (litigation privilege).

'Dawn raids' in the antitrust sector

Regulators in a number of sectors benefit from powers of entry and inspection. In this article, we consider the extent to which the 'dawn raids' powers of the EU and UK antitrust authorities resemble the ICO's enhanced powers of inspection. Under UK competition law, unannounced inspections can be carried out both with and without a warrant (in the latter case, the Competition and Markets Authority ("CMA") cannot search the premises but can require documents and other information to be produced to it). Under EU competition law no warrant from a court is required.

In relation to the time of entry, the CMA can enter under warrant at any time but if there is no-one at the premises the CMA needs to offer the occupier (or their legal representative) a reasonable opportunity to be present when the warrant is executed. However, the CMA can effectively only enter without a warrant during business hours (since it is unable to search premises without a warrant and therefore requires personnel to be on the premises). While EU competition law is silent on the timing of dawn raids, they will typically take place during business hours so that relevant documents and other evidence can be located following consultation / questioning of personnel.

The same principles relating to legally privileged information apply under relevant UK competition law. However they are more widely cast to include all types of privileged communications (not simply those relating to competition law legislation). EU privilege rules will apply in respect of dawn raids carried out by the European Commission and are narrower, notably not including advice from internal counsel.

The similarities between the ICO's enhanced powers to enter and inspect premises and the 'dawn raids' powers of the CMA and European Commission are such that, despite some of the differences referred to above, businesses can still take advantage of the learnings and experience from the antitrust sector.

Preparing for an ICO inspection - some practical considerations

Businesses have for some time reflected competition law enforcement powers in their internal compliance manuals and procedures. Similar considerations are applicable in respect of the ICO's new powers under the DPA 2018 relating to inspections with little or no notice. Helpfully, many of the processes set out in a business' data breach plans will also be relevant.

Given the criminal liability (as well as wider reputational damage) attaching to failures to cooperate with the ICO in the context of an inspection, it is important that businesses take steps to prepare themselves for the possibility of an inspection with limited or no notice by the ICO.

Actions to take to prepare for an ICO inspection

Compliance procedures

Update data protection compliance procedures and/or competition dawn raid guidelines or create new ones covering the ICO's powers, to reflect the fact that the ICO can carry out unannounced inspections.

Core team

Establish a core team of key individuals that will be on the 'front-line' of any ICO inspection. Of particular importance will be individuals connected with the data management functions of the business, including those with knowledge of the business' data storage systems. Such a team could include, for example, the Data Protection Officer/Head of Privacy, members of senior management, relevant IT staff, and internal and external legal counsel. This is likely to be the same team that would be convened under any data breach response plan.

Clear reporting lines

Agree and document clear reporting lines, starting from the moment an unannounced inspection commences (including for example a 'cascade list' of key contacts, and key roles and responsibilities for staff) or notice of an imminent inspection is received. Such reporting lines should cover not only the internal conduct of the business during and after an inspection, but also liaising with the comms team to manage external publicity.

Internal training

In readiness for an ICO inspection, train relevant staff on how to conduct themselves, and who to contact and when. It is particularly important to train receptionists and front desk staff as they will be first in line. Consider simulating an inspection to verify that the business' procedures are sufficiently well-organised to minimise the disruption that might arise.

Template responses

Prepare emails to relevant employees advising that an inspection is underway (and what actions they need to take or not take e.g. holding back from mentioning on social media or anywhere else that an inspection is underway) and any other template documents that should be distributed quickly (e.g. document preservation notices or inside information announcements).

Appoint legal counsel

Appoint external legal counsel in advance so that conflicts and other issues are already cleared. There is a need to ensure close legal scrutiny of the ICO's conduct during unannounced inspections (e.g. to ensure that legal privilege and procedural requirements are respected). It may also be possible to challenge certain aspects of an on-notice inspection (e.g. the urgency of any notice).

Documentation

Ensure all privacy compliance documents are easily accessible, in particular the businesses records of processing, breach log and relevant data protection impact assessments and policies.

In practice, the actions above will be relevant for both unannounced and on-notice inspections. Obviously, the shorter the notice period, the more important it will be to have taken as many of these steps as possible in advance. If that has not been possible, it will be important to prioritise. In particular, businesses should focus on setting up a core team of individuals, getting the legal team on-board, establishing clear lines of reporting and ensuring all relevant information is to hand to show to the ICO. In some cases, where the reason for an inspection is unknown to the business, it will be necessary to carry out an internal investigation in parallel to the preparations for the inspection. This should follow the business' data breach response policies and protocols. Further details on this can be found on our **publications** on data breaches.

How likely is it that ICO will carry out an unannounced inspection?

In practice, it is unlikely that the ICO will regularly be carrying out inspections with little or no notice. Unsurprisingly, the thresholds for obtaining a warrant for these types of inspection are harder to meet than where a longer notice period has been provided. They are also resource-heavy operations, not least because they will often need to cover a number of sites or premises at the same time to be effective. Unless the ICO is dealing with a very public and/or high profile potential breach, and/or it has sufficiently strong evidence such as a whistle-blower's witness statement, it may struggle to obtain sufficient information to satisfy a judge there are reasonable grounds for suspecting breaches of the specified data protection legislation or that offences have been committed.

In addition, the ICO has typically tried to co-operate with organisations, at least in the first instance, when taking regulatory action. This is reflected in its draft Regulatory Action Policy which states that, "*as a general principle, the more serious, high-impact, intentional, wilful, neglectful or repeated breaches can expect stronger regulatory action. Breaches involving novel issues, technology, or a high degree of intrusion into the privacy of individuals can also expect to attract regulatory attention at the upper end of the scale*." The consultation on this draft closed on 28 June and at the recent PL&B conference in Cambridge, an ICO spokesperson commented that the ICO hopes to publish the final version over the summer.

However, it is difficult to predict the media coverage and reaction to a breach and, as the Cambridge Analytica investigation has shown, the ICO will make use of its strongest powers where appropriate. Businesses should therefore put in place the recommendations above now to ensure they are prepared for the ICO making use of its varied powers of inspection.

Slaughter and May advises on all aspects of data protection and privacy. If you would like further information, please contact Rebecca Cousin, Jordan Ellison or your usual Slaughter and May advisor. All our data protection and privacy publications are available on our ***website****.*

Jordan Ellison
T +32 (0)2 737 9414
E jordan.ellison@slaughterandmay.com

Alexander Chadd
T +32 (0)2 737 9419
E alexander.chadd@slaughterandmay.com

Rebecca Cousin
T +44 (0)20 7090 3049
E rebecca.cousin@slaughterandmay.com

Richard Jeens
T +44 (0)20 7090 5281
E richard.jeens@slaughterandmay.com