



Karolos Seeger, Jane Shvets, Robert Maddox.

Beyond the headline fines: preparing for post-GDPR ICO scrutiny and enforcement

29 October 2018

*As fines grab the headlines, Debevoise & Plimpton London partners **Karolos Seeger** and **Jane Shvets** and associate **Robert Maddox** analyse the UK data protection watchdog's new investigative powers.*

With the entry into force of the GDPR, several EU member states have updated their local legislation to grant their data protection authorities enhanced investigative and enforcement powers. Some authorities, such as Ireland's Data

Protection Commission, have been given the ability to impose civil fines for the first time. Although the UK Information Commissioner's Office (ICO) has had the ability to impose fines for years, the maximum amount has grown exponentially. As those fines grab the headlines, it is important to appreciate the extent of the ICO's new and pre-existing investigative powers, which enable it to investigate UK-based companies and impose those hefty penalties.

This article explores two key investigative powers in the ICO's enforcement armoury – information notices and assessment notices. It then considers the lessons from other enforcement areas where regulators have exercised similar authority for years.

Information Notices

An information notice is a request that the ICO can issue to a data controller, data processor, or another party, seeking specified information by a specified date in connection with an ICO investigation. By default, an information notice must give the recipient at least 28 days to provide the requested information. The ICO can also issue an urgent information notice in certain circumstances, requesting information in as little as 24 hours. If the recipient does not respond or does not respond fully in the allotted time, the ICO can seek a court order to enforce the notice. The ICO has indicated that it will do so “promptly” in all but exceptional circumstances.

The speed of the response should not detract from its accuracy, however; knowingly or recklessly making materially false statements in response to an information notice is a criminal offence. So is destroying, disposing of, concealing, blocking access to, or falsifying relevant information (or causing or permitting another to do the same) upon receipt of an information notice, unless the company can show that those steps would have been taken had the notice not been received.

While an information notice is unlikely to be the ICO's default method of obtaining general information from businesses regarding GDPR compliance, they will certainly constitute the ICO's first investigative step where it has identified material concerns about such compliance. They will be used, at the ICO's discretion, when

there is high risk of harm to individuals, such as risk of intrusion into their private lives; there is a demonstrable benefit to requiring the recipient to provide information by the given deadline; an information notice is likely to improve the likelihood of receiving accurate responses; and/or issuing the information notice is in the public interest.

The exercise of responding to information notices is undoubtedly going to test companies' compliance with the GDPR's record-keeping requirements. Companies are therefore well advised to get their house in order with respect to requirements and the GDPR's overarching accountability principle, which requires them to be able to demonstrate compliance. The threat of a potential information notice and the prospect of follow-on ICO investigations, including an Assessment Notice, or fines in the event of an inadequate response to such notice should provide a strong incentive for immediate remedial action.

Assessment notices

As onerous as they may sound, information notices are a relatively light touch when compared with the newly updated tool in the ICO's arsenal: the power to issue what can only be described as intrusive assessment notices. An assessment notice can require a data controller or processor to grant the ICO access to its premises, requested documentation, information, and equipment, and to make personnel available for interviews by the ICO. Assessment notice powers are deliberately broad, and designed to enable the ICO to gather all the information it needs to determine whether the GDPR or UK Data Protection Act 2018 (UK DPA) have been violated.

The ICO has indicated that it will consider the following factors in deciding whether to issue an assessment notice: the probability that personal data is currently processed in violation of the law, taking into account the existence of communications, news reports, or other information suggesting that is the case; whether issuing an assessment notice is necessary to verify compliance with a prior enforcement notice; and whether the recipient previously has failed to respond to an information notice. It is likely, therefore, that assessment notices will be limited to cases of suspected or confirmed serious violations of data processing

requirements or situations where the recipient has failed, or might have failed, to comply with a prior investigatory or enforcement action, as was the case in the recent Cambridge Analytica investigation.

Assessment notices can cover not only the documents physically located in a company's UK office, but also data held elsewhere, as long as it is remotely accessible from the equipment on the UK premises. This is a significant extraterritorial element of the ICO's powers, which may give the ICO broader access to data held outside of the UK than that available to other UK law enforcement and regulatory agencies. This aspect of assessment notices gives companies another reason to think critically about their IT infrastructure and how they set up cross-border remote access to data spread across jurisdictions.

As with information notices, the default period to comply with an assessment notice is 28 days. That can be reduced to seven days, or even to immediate compliance with the ICO, where it has reasonable grounds to believe that is necessary to prevent an ongoing violation. For companies that process significant quantities of personal data or otherwise can be deemed higher risk from a data protection compliance perspective, figuring out the practical assessment notice compliance steps can be a worthwhile exercise.

Lessons from other regulatory contexts

In many respects, the ICO has only recently hit its stride by gaining additional investigative powers, the ability to collect very significant post-GDPR fines, and capitalising on the public attention paid to data privacy matters. As the ICO's enforcement practice grows, companies would be well advised to learn from other regulators' investigative practices.

First, proactive engagement and cooperation with the ICO is likely to be advisable. Anyone familiar with the corruption investigations that have grabbed the headlines in recent years will be well acquainted with the concept of cooperation credit, and its potential effect on the form of the corporate resolution and resulting fines. The UK DPA explicitly recognises that the extent of a company's cooperation will be a factor in setting penalties. A cooperative stance may also obviate the need for more intrusive investigative action. In the same way that responding to a voluntary


request from anticorruption authorities may stave off the issuance of a subpoena, sharing information with the ICO on a voluntary basis may spare the company an information or assessment notice and allow for a more flexible and productive information exchange.

Second, like in the investigations by the UK's Serious Fraud Office (SFO), ICO investigations are likely to implicate legal privilege issues, although in a different way. Unlike section 2 of the Criminal Justice Act 1987, which sets out the SFO's powers and incorporates the common law standard for privilege, the UK DPA contains its own definition of legal privilege, which may in some cases be at odds with its common law counterpart. For example, the UK DPA states that legal privilege applies to documents produced "for the purposes" of actual or contemplated proceedings. It is not clear whether that is intended to be different from the common law's "dominant purpose" test, which is arguably narrower. In addition, the UK DPA's formulation of legal advice privilege suggests that it applies only where the communications at issue involved legal advice provided under the GDPR or the UK DPA and limited other laws, but not the Data Protection Directive or previous Data Protection Act. As the ICO's investigations gain momentum, these uncertainties may become a source of privilege disputes, similar to the one that played out between the ENRC and the SFO.

Third, the ICO will not regulate in a vacuum. It shares information with data protection authorities in other countries, both in and outside of the EU, and will in some cases coordinate its investigative and evidence-gathering activities with overseas partners. The ICO will also work with other UK regulators, including the Financial Conduct Authority (FCA). This inter-agency and cross-border cooperation may lead to the same "piling on" concerns that have been raised in the context of multijurisdictional corruption settlements. Breaches of the GDPR or the UK DPA can also constitute breaches of a regulated entity's FCA obligations, or of other countries' data protection or other legislation. As more regulators and countries turn their attention to data breaches and other data protection matters, it is likely that the difficult question of "dividing up" an investigation, and apportioning any resulting fines, will come up, notwithstanding the GDPR's one-stop-shop mechanism for intra-EU issues.

Conclusion

Time will tell how broadly and aggressively the ICO will use its investigative and enforcement powers. Early indications – including the ubiquitous “ICO Enforcement” windbreakers seen in the context of the Cambridge Analytica investigation, and the reports of ICO’s investigation into the validity of cross-border data transfers – are that the ICO’s enforcement will ramp up. All businesses, and especially those that deal with significant quantities of personal data, should prepare for the advent of a new proactive regulator and enforcer.

 Data privacy, Enforcement

Copyright © Law Business Research Company Number: 03281866 VAT: GB 160 7529 10