October 26, 2020

ICO Draft Statutory Guidance on Regulatory Action

Attorneys
Rohan Massey
Clare Sellars

The Information Commissioner's Office (ICO) has published for consultation its draft "Statutory guidance on our regulatory action" detailing how it will exercise its regulatory functions when issuing information notices, assessment notices, enforcement notices and penalty notices. The document sets out the ICO's risk-based approach to taking regulatory action against organisations and individuals that have breached data protection law. The ICO's focus is on the areas of highest risk and most harm. The guidance sets out the principles the ICO will apply along with details of the nature of the ICO's various statutory powers and how it will exercise them in a "fair, proportionate and timely" manner to guarantee that individuals' rights are properly protected. It also sets out how the ICO will deal with privileged communications. The consultation closes on 12 November 2020.

Information notices

An information notice is a formal request under s 142 of the DPA 2018 for a data controller, processor or individual to provide the ICO with information, within a specified time frame, to assist it with its investigations. As the draft guidance explains, the ICO will serve an information notice at its discretion according to what it considers is appropriate and proportionate, including risk of harm to individuals or the level of intrusion into their privacy potentially posed by the events or data processing under investigation. Among other things, a further key criterion is the public interest in the response.

Additionally, when deciding the period for compliance with an information notice and whether to issue an "urgent" information notice, the ICO will consider, amongst other things, the extent to which urgent investigation may prevent or limit the risk of serious harm or serious intrusion and, in particular, the extent to which it may prevent the alteration, destruction, concealment, blocking, falsification, or removal of relevant evidence of data processing.

If a recipient of an information notice fails to respond within the applicable time the ICO can apply for a court order requiring a response. Whether it does so will depend on the reasons for non-compliance, any commitments that may have been given, what evidence is to hand and whether it may be obtained from another source, and the public interest. Ultimately, however, the ICO may consider issuing a penalty notice.

Assessment notices

The ICO can also issue assessment notices under s 146 DPA 2018 to data controllers or processors to allow the ICO to consider whether they are compliant. The notice may, for example, require that the ICO be given access to premises and specified documentation and equipment.

An assessment notice might be issued in various circumstances, (for example, where it is necessary to verify compliance with an enforcement notice, or the controller or processor has failed to respond to an information notice within an appropriate time. Depending on various factors, such as the extent to which urgent investigation may minimise the level of potential risk of harm to individuals or intrusion into their privacy, or risk of interference with evidence, as well as, amongst other things, the impact on the rights of the recipient of such a notice, the ICO might issue an "urgent", "no-notice" or "short-notice" assessment notice.

Again, if an organisation fails to respond to an assessment notice, the guidance notes that the ICO will consider seeking a court order to force that organisation to supply the information requested, or applying for a warrant to gain access to premises to access the information, or issuing a penalty notice.

The guidance states that, among other things, the ICO may require access to specified documents and information which indicate how organisations have complied with the legislation and what governance measures are in place to monitor compliance (e.g. strategies, policies and data protection impact assessments). The ICO notes that it will access the

minimum amount of information necessary to assess whether an organisation is handling personal data appropriately. However, it might require access to information which is subject to legal professional privilege, is highly commercially sensitive or is exempt from the DPA 2018 in the interests of national security. In respect of information regarding national security, international relations or sensitive activities, the ICO says it will try to assess compliance without looking at this type of information, if possible and will also try to minimise access to health and social care records.

Inspections and examinations are considered key review elements of an ICO assessment which help the ICO identify objective evidence of how an organisation is complying and implementing data protection policies and procedures. In its review of personal data, and associated logs and audit trails, the ICO may consider both manually and electronically stored data. It will also consider management/control information and physical and IT-related security measures, including how the data controller stores and disposes of personal data. Review and evaluation may be carried out on site as part of discussions with staff, or independently through sampling, and controllers may be asked to provide manual copies of or arrange direct access to electronic information.

The ICO may conduct interviews during assessments with staff and contractors, as well as staff of relevant processors and service providers which seek to understand working practices and/or awareness of regulatory obligations and individual roles and processes followed or managed, specifically in relation to the handling of personal data and its security.

The ICO will conclude its assessments in most cases with an audit report setting out its conclusions and any recommendations to address weaknesses or compliance issues that have been identified. The ICO may decide no further formal action is needed, but may share copies of the report internally to decide what action to take and will confirm its decision to the organisation. It will also publish executive summaries of audit reports on its website.

Enforcement notices

The ICO may issue enforcement notices under s 149 of the DPA 2018, for example, where a data controller or processor has breached one of the data protection principles. Their purpose is to mandate action or, for example, prohibit further processing, in order to bring about compliance, remedy a breach or both. Failure to comply may lead to further action, including possible penalty notices.

The guidance explains that enforcement notices will usually be appropriate where there has been a repeated failure to meet information rights' obligations or time scales, there are serious ongoing infringements to individuals' rights and freedoms, or where the processing or the transfer of information to a third country fails to meet the requirements of the DPA 2018 and GDPR (among other circumstances). Aggravating or mitigating factors will also be considered.

The ICO explains that time scales set out in an enforcement notice will usually reflect the imminence of proposed action, the severity and scale of any breach or failings, and the feasibility of correcting measures or technology. Again, the ICO could issue an "urgent" enforcement notice depending on various factors.

Penalty notices

Ultimately, the ICO may issue penalty notices under s 155 of the DPA 2018. These set out the ICO's intention to fine an organisation for any breaches of data protection law with the aim of punishing that organisation, promoting future compliance and acting as an effective deterrent.

The guidance states that, in most cases, the ICO will issue penalty notices for the most serious breaches of information rights obligations, such as those involving intentional or negligent acts, or repeated breaches, or causing damage to individuals. The ICO will be more likely to impose a penalty in various circumstances, for instance, where many individuals have been affected, where there is a degree of damage (which can include embarrassment and/or distress) or where special category data has been involved. Penalty notices are also likely where there has been a failure to comply with an information notice, an assessment notice, or an enforcement notice, or there has been a repeated breach of

obligations, or a failure to rectify an identified problem, follow ICO recommendations, or apply reasonable measures to mitigate any breach. Intentional non-compliance is also likely to attract a penalty notice.

Nevertheless, before issuing a penalty, the ICO will issue a Notice of Intent (NOI) informing the recipient that the ICO intends to serve them with a penalty and setting out its rationale for doing so and the proposed amount. The recipient will be given at least 21 calendar days to make written representations about the imposition of the penalty and the proposed amount, which the ICO will consider. Organisations may also be allowed to submit representations verbally in exceptional cases. The ICO will also consider representations from any other Concerned Supervisory Authorities in deciding the final amount of any penalty. For substantial penalties, a panel of non-executive advisers to the ICO may be convened.

The draft guidance also sets out the ICO's approach to the calculation of administrative penalties under ss 155 to 157 of the DPA 2018 and Article 83 of the GDPR. The maximum amount of any penalty will depend on the type of breach and whether the "standard maximum amount" or "higher maximum amount" applies. The higher maximum amount is, in the case of an undertaking, €20 million or 4% of turnover, whichever is higher, or in any other case, €20 million. The "standard maximum amount" is, in the case of an undertaking, €10 million or 2% of turnover, whichever is higher, or in any other case, €10 million.

The ICO explains that where a fine based on turnover exceeds the €10 or €20 million limit, it will cap the fine at the relevant limit. It may impose a fine up to the relevant limit, if a fine based on turnover would not result in a proportionate fine because, for example, a company has a very low or no turnover, but is guilty of a serious breach. Where the ICO is able to decide the amount of any penalty in the context of its regulatory work, the guidance notes that this will be based on a nine-step mechanism within the legislative limits. Ultimately, the calculation will depend on, among other things, the seriousness of the contravention, the degree of culpability, the ICO's determination about turnover, any aggravating or mitigating factors, the economic impact of the fine and the effectiveness, proportionality and dissuasiveness of any penalty.

Other matters

The draft guidance also covers fixed penalty notices that the ICO can issue under s 158 DPA 2018 for failing to pay the required data controller registration fee to the ICO (such fixed penalties range from £400 for tier 1 (micro) organisations to £4,000 for tier 3 (large) organisations).

The guidance also includes information regarding the ICO's treatment of privileged communications, how the ICO will ensure that these will only be used or disclosed to the extent required to carry out the ICO's functions and also how the ICO will comply with restrictions or prohibitions regarding the obtaining or accessing of privileged communications.

Comment

The draft statutory guidance helps data controllers and processors understand what action may be taken against them and in what circumstances following a suspected breach, and ultimately, following the determination that a data breach or other event of non-compliance has occurred, including failure to implement adequate security measures or comply with transparency obligations. The document reaffirms the ICO's "follow the money" approach to enforcement. However, there is a strong public interest element and smaller organisations should be wary of deriving a false sense of security from the ICO's "risk-based approach" to taking regulatory action, since this can encompass not only the actual impact of the infringement in question, but also its potential significance for the public at large. This might arise, for example, as a result of the unauthorised use, even on a small scale, of certain technologies and the processing of sensitive personal data, facial recognition technologies being an obvious example.