Regulatory investigations by the UK ICO Part 2: procedural steps and preventive measures

In Part 2 of this multi-part series on ICO investigations, Liz Fitzsimons, Partner, at Eversheds Sutherland LLP, outlines the procedural steps of a typical investigation and highlights measures for minimising the risk impact

In Part 1 of this series of articles, we considered the current approach taken by the Information Commissioner's Office (ICO) in relation to investigations, and explored the main areas of breach that are liable to attract the regulator's attention.

In Part 2, we look in detail at the procedural steps of an ICO investigation together with further preventive measures to minimise the risk to an organisation from such an inquiry.

New ICO regulatory policy and methodology

The ICO last confirmed its regulatory approach in November 2022, linked to its ICO25 strategy. A key takeaway from its foreword is that the ICO 'will not hesitate to take steps to protect people from the unscrupulous who wish to cause harm, or those who are reckless and seek to avoid their responsibilities.' The details also confirm that the ICO will 'take a risk-based approach to regulatory action' and that its focus is 'usually on areas of high risk where non-compliance could do the most harm.'

The ICO will use its 'formal enforcement actions when necessary to protect people and prevent harm' but has been testing different approaches, such as reducing the impact of fines on the public sector, as this 'often also impacts the victims of the breach, by reducing budgets for vital services'. As a result, when dealing with public bodies, the ICO has been increasing 'the use of public reprimands and enforcement notices' and 'only issuing fines in the most egregious cases'.

The impact of action on private businesses and the economy is also considered in ICO regulatory decision-making. Although each case is considered on its own facts and merits, the ICO's prioritisation framework considers multiple factors, such as:

- the likely impact of ICO action, taking account of risks, harms and opportunities to improve compliance;
- alignment with ICO strategic priorities (including whether collaborative enforcement through another regulator may be better);
- probable successful regulatory outcomes and whether these are consistent with ICO aims; and
- required resources to achieve the outcomes.

Perceived and evidenced risks of harm are key to the ICO approach, which assesses evidence of harm, the degree of public concern, the likelihood of success from intervention, and the legal, financial, and reputational risks involved.

The ICO's approach is dynamic and its policy is clear that this will be kept under review with flexibility in the approach to accommodate new developments and challenges.

The ICO issued its new methodology in February 2024. Of particular interest is how the ICO's regulatory policies and related decision-making are affected by its work on the 'taxonomy of harms,' taking into account potential harms to people, and the ICO's related Impact Assessment Framework, its use and completion of impact assessments by the ICO. This is key to the development of the ICO's Regulatory Policy and this in turn drives it approach to regulatory investigations, their prioritisation, outcomes and related publicity.

On 18 March 2024, the ICO announced a change in how it will decide to issue penalties and calculate fines, and the ICO website indicates that further changes affecting other types of regulatory investigation and enforcement should be expected.

The ICO's process for regulatory investigations

The ICO will allocate a relevant case/investigatory officer to consider the issues and lead any investigation. It will first obtain details about the alleged non-compliance independently, for example from the complainant, another third party, or from its own checks.

The ICO's revised approach to its

regulatory investigations has been most evident in its changes to investigations in relation to public access information request complaints (although its approach and procedure in such cases is currently under review and expected to change still further).

Sifting process and assessment of priority

An ICO sifting process ensures complaints received are screened and allocated to the correct team, dependent on their subject matter and the relevant legal regime. The complaint may in some cases also be allocated to a relevant sectoral queue, which helps the ICO to spot common issues and trends, e.g. complaints affecting the police, or health or education related organisations. The ICO operates sectoral databases of complaints and issues. Even if your organisation has not yet been affected, the ICO will have in mind relevant sector issues and practices if your organisation comes to its attention.

The next step is for the details to be assessed for prioritisation, early resolution, and/or assessment as to whether it is connected to other cases. An appropriate case officer is allocated to deal with the case (or connected cases).

Identifying the basis of the complaint

The basis for the complaint must be clear from the details provided by the complainant, especially in public access to information cases, as the 'case officers will not go through correspondence to construct complaints'. The case officer may liaise with the complainant 'to clarify the complaint or to provide specific documents relevant to the request', although the ICO will expect this to be done promptly and normally within 28 days at most. Ineligible complaints will be rejected and the matter closed.

> ***"The ICO expects organisations to use the advance warning about a complaint... such notice period must be used wisely to get on top of the allegations and relevant facts, gather all relevant details and to assess the compliance position and how best to deal with the investigation and claims"***

Complaints identified as eligible will trigger the ICO's process and use of its template communications to update the complainant and to notify the affected organisation that the complaint is being dealt with. The regulator will also indicate when the organisation is likely to be contacted in respect of the investigation.

A pre-allocation communication to the organisation explains the kind of information the case officer will require and why, and advises the body 'to prepare and collate relevant documentation.'

Advance warning

The ICO expects organisations to use the advance warning about a complaint to ensure that it is clear about what information the complainant has asked for, what information the organisation holds, what it has provided, and what has been withheld, and to have this ready for the follow on case officer contact.

Any such warning period must be used wisely to get on top of the allegations and relevant facts, gather all relevant details and to assess the compliance position and how best to deal with the investigation and claims. This opportunity may not be available in all cases, especially those where the ICO is concerned about the safeguarding of evidence and wants to ensure that relevant details of non-compliance cannot be destroyed.

Liaison and suggested next steps

Following this, in most cases, once the details have been considered by the ICO and a preliminary view has been formed, the allocated case officer will then liaise with your organisation about what they have been told, what they think and what they need your organisation to do. The approach here will vary widely dependent on the relevant legislation and issue.

The ICO's approach will be dependent on whether the regulator believes that the issue is suitable for early resolution. This involves cases needing no or minimal investigation, such as where there is a 'clear precedent' setting out the ICO's existing position on the requested information (when the ICO will simply issue its decision notice), or where ICO's views would be shared with the organisation and complainant quickly and, in some cases, the decision reached without the need for direct contact.

Submission to respond

If the case is not suitable for early resolution, or this has been attempted unsuccessfully, a full investigation will be undertaken and the organisation will be asked 'to reconsider the case and provide a submission' to respond 'to the issues raised' and may be asked to answer specific questions posed. The ICO warns that it expects organisations contacted 'to engage positively … provide relevant information in a timely manner and at the first time of asking.' The submission should cover 'how you handled and responded to the request; where applicable, why an exemption or exception applies; … [and in relevant cases] how the public interest in maintaining that exemption [or exception] outweighs the public interest in disclosure.'

The submission must be prepared on the basis that the ICO explicitly wants the organisation to recheck

(Continued on page 8)

(Continued from page 7)

its reasoning by considering relevant ICO guidance (general and specific) and relevant decision notices the ICO has issued (notwithstanding that these are case and fact specific and do not form legal precedent).

ICO commentary suggests that 'it will be useful' if the submission includes relevant contextual and background information, sufficient to ensure that the ICO can understand relevant sensitivities, copy supporting documentation and the views of the organisation on whether it is open to adjusting its position (such by making additional disclosures), or any informal resolution. The ICO is always keen for parties to resolve issues without the need for regulator involvement if that seems possible at any stage.

When providing its submission to the ICO, it should be noted that the organisation is encouraged to provide to the ICO any supporting legal advice that it has received. Although the ICO has noted that there is no obligation to provide such advice to it, careful consideration is needed before any such submission is made, (in case legal privilege is inadvertently waived and lost), and as to how such submission is made, in order to minimise related risks. Although the ICO is also keen to understand the names and roles of staff involved in dealing with relevant cases, great care is also needed about the provision of these sort of details due to the potential risk of the ICO wishing to name and shame relevant personnel in some cases.

Timing expectations

The accelerated timing expectations of the ICO are clear from its guidance which confirms that normally the authority will have ten working days to make its final submission, with the deadline being clearly indicated. The deadline will be case and fact specific, with due consideration of the relevant volume and complexity of information and the case officer is more likely to set a shorter deadline for early resolution cases. Failing to respond within the deadline is not recommended, and furthermore you should always try to agree a deadline that your organisation can meet, and proactively warn the ICO about any unexpected delays.

> ***"Failing to respond within the deadline is not recommended, and furthermore you should always try to agree a deadline that your organisation can meet and proactively warn the ICO about any unexpected delays"***

Although the case officer should check whether there is a good reason for the delay and, where this can be properly explained, is likely to agree a 'reasonable' extension, if the ICO does not obtain a satisfactory explanation or update, it may issue a formal information notice escalating the importance of the need to comply and on time. If your organisation does not respond to the ICO's enquiries, the ICO is entitled to make its decision 'purely on the information already submitted,' which the ICO acknowledges means that your organisation is 'more likely to receive an adverse decision notice.' It is therefore critical that your staff are aware of these risks, well trained to spot relevant communications, and able to ensure they are dealt with as required by the ICO and in good time.

Resolution

If the ICO indicates no case to answer to the complainant, or if the matter is informally resolved and the complainant agrees to withdraw their complaint, the case will be closed by the ICO and no decision notice issued. In all other cases (unless the ICO has determined the complaint to be 'frivolous or vexatious,' which would be very rare), the ICO will proceed to issue a decision notice.

It should be noted that ICO senior managers may identify cases as involving high profile issues, in which case they are logged and their investigation and resolution 'may be prioritised or escalated'. Any such cases are more likely to result in ICO driven publicity. This is also likely where complaints have been submitted by elected representatives, or where a complaint is the subject of media coverage.

For complaints relating to information law requests, the ICO is committed to resolving 90% of them within six months of receipt and all of them within twelve months of receipt.

In relation to self-reporting of personal data breaches, how well the breach has been dealt with and contained and, in particular, how well the initial reporting has been handled is critical to the next steps by the ICO and how concerned they will be. We have regularly seen how a combination of good data practices and strong notifications can result in ICO confirmation of no further action required, even where breaches affect a probable high risk area for the ICO, such as the health sector.

Increasingly for other data protection breaches, single complaints may well generate some broad (and possibly unhelpful) compliance commentary from the ICO and require further steps by your organisation direct with the data subject or complainant, with the ICO pushing resolution of the matter back down to your organisation. Bearing in mind that, in many cases, data subjects have legal rights to claim compensation for loss caused by non-compliance, there may be additional unwanted complications flowing from any such determination shared with affected individuals.

In more serious data protection cases, or where direct resolution of a specific complaint has still not been possible, the ICO will pursue a more detailed investigation and may well make further demands of your organisation. The ICO expectations explained above will be helpful to keep in mind even in these cases.

Patterns, heat maps and hot spots

It is important to remember that the ICO will build up a picture about alleged compliance practices in your organisation based on the number of complaints raised, over what period and their overlapping or varied subject matter. These, together with what the ICO finds when investigating such complaints, leads it to build up a 'heat map' about your organisation, identifying areas which appear to be non-compliant as 'hot spots' (too many similar complaints and within a limited period), attracting greater ICO scrutiny and causing the most concern.

Where a hot spot is identified by the ICO and determined to be getting too 'hot', the ICO is likely to take proactive action, may place the organisation under more onerous monitoring or assessment regimes, and if the ICO's regulatory investigation(s) show what it views as serious, repeated non-compliance (and especially if it believes there are systemic or major organisational issues with compliance), the regulator is highly likely to escalate its approach to enforcement activity, publication and publicity.

"When self-reporting breaches, or providing information to regulators…your organisation should always assume that they will share information with each other...Your organisation must ensure that it is consistent in what it says to all parties, as accidental or deliberate differences will be noted and dealt with appropriately"

Additional risk factors for regulatory investigations

The more press and public interest in an issue, the greater the number of individuals affected, the more important the issue and/or affected organisation (whether due to its sector e.g. the police, seniority e.g. central government, or its size and brand), the more likely it is that details will be publicised by the ICO.

Your organisation should also be extremely aware of the core focus areas of the ICO in its current strategy and related objectives (ICO25 strategic plan), including:

- safeguarding people;
- promoting openness, transparency and accountability; together with
- the ICO's current key priorities:
  - ♦ AI in recruitment;
  - ♦ child protection;
  - ♦ financial services;
  - ♦ extraction of mobile phone data related to criminal justice; and
  - ♦ auditing compliance with electronic privacy laws.

Issues touching any of these topics are far more likely to attract ICO attention, higher priority treatment and scrutiny, and to drive regulatory investigation, related outcomes and publicity.

The UK's ICO is definitely not an island

It is really important to know that the ICO does not operate in isolation.

The ICO is well-versed in collaborative working with other regulators and bodies, with strong co-operative and information sharing relationships set up between them (often based on a published Memorandum of Understanding), such as with the Care Quality Commission, Charity Commission, Competition and Markets Authority, Financial Conduct Authority, the National Cyber Security Centre, National Crime Agency, Ofcom and Ofgem.

The regulator notes that 'subject to information sharing restrictions in relevant legislation, we share intelligence, threat analyses, insight and tactics with these organisations. We also refer relevant cases if they fall within their jurisdiction as well as our own. Where we undertake joint regulatory or investigative work, we coordinate our activity'.

These connections are not limited to UK bodies and regulators but also include those with many equivalent overseas regulatory bodies, including the European Data Protection Supervisor and the US Federal Trade Commission. Although (following the UK's exit from the European Union) the ICO is no longer a representative member of the European Data Protection Board (EDPB), the ICO and the EDPB maintain good working links.

When self-reporting breaches, or providing information to regulators, law enforcement bodies or similar, your organisation should always assume that they will share information with each other. The ICO will obtain details from other regulators with whom they will similarly share information. Each entity will cross check the details it receives direct. Your organisation must ensure that it is consistent in what it says to all parties, as accidental or deliberate differences will be noted and dealt with appropriately.

What your organisation needs to do

Your organisation must be ready for the ICO's contact when it gets in touch to take forward its investigation, and should be prepared to deal with the regulator's questions and demands quickly and thoroughly.

What is clear is that your organisation may now only have a single opportunity to put forward its defence to the investigation. That opportunity must be used wisely and not wasted. Failure to do so is likely to lead to worse outcomes for the organisation, such as a greater risk of damaging

(Continued on page 10)

(Continued from page 9)

publicity and increased costs from the need to escalate the issues through legal challenges in some cases.

Ideally, your organisation must consider the before, during, and after, periods for any regulatory investigations which may impact it.

- Is your organisation on top of its compliance and related record keeping?
- Can your organisation evidence its compliance – what is documented and is this up to date?
- Can it prove why staff are aware of their obligations?
- Can it prove what happened in specific cases and how the organisation met its obligations?
- Will all its communications with people evidence good compliance practices?
- Will it be able to obtain all the details needed quickly, in order to provide them to the ICO in response to any regulatory investigations?
- Does your organisation know whether it has been affected by previous similar breaches or complaints?
- If similar breaches have occurred, does your organisation know their outcomes?
- Has the organisation considered lessons learned from previous breaches or complaints and made appropriate improvements that can be evidenced?
- Have all reasonable appropriate steps been taken to ensure that the organisation is compliant and meets its obligations?
- Can your organisation prove all of this to the ICO?

The greater the number of positive responses to these questions, the better placed your organisation is to respond to an ICO regulatory investigation and to obtain a positive outcome. The lower the number of 'yes' answers, the greater the risk of an adverse outcome and negative publicity.

A good rule of thumb is to consider how you personally would react if forced to explain your compliance approach to a specific case to the actual Commissioner, face-to-face. If the explanation of your organisation would make you blush, you know that there is more work to do.

In Part 3 of this series of articles, in *Compliance & Risk* Vol 13 Issue 4, we will explore the latest data protection fining guidance issued by the ICO, considering what this means for practitioners and organisations, and how the ICO approach to penalties compares to that of other regulators.

Liz Fitzsimons

Eversheds Sutherland LLP

liz.fitzsimons@eversheds-sutherland.com