ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Inside the ICO's new enforcement toolkit: Breaking down the draft guidance

Organisations should pay attention to the ICO's new settlement procedure and expanded information gathering powers. By **Alison Llewellyn** and **Katie Hewson** of Stephenson Harwood.

The UK Information Commissioner's Office (ICO) has recently closed its consultation on new draft Data Protection Enforcement Procedural Guidance (the Guidance), which sets out in detail how the ICO intends to use its investigatory and enforcement

Continued on p.3

When an incident is just the tip of the cyber iceberg

Richard Jeens and **William Doyle** of Slaughter and May reflect on lessons learned from ICO enforcement in 2025 and key developments for 2026.

Last year, 2025, revealed a shift in enforcement approach by the Information Commissioner's Office (ICO) when compared to the previous year. We saw a decrease in overall enforcement action, but a much higher proportion of those actions taken against organisations in the private sector and a significant focus on cyber and data security failings. This comes amid high-profile cyber-attacks against

Continued on p.5

Issue 144 **MARCH 2026**

See the publisher's blog at privacylaws.com/blog2026mar

UNITED KINGDOM
report

ISSUE NO 144 **MARCH 2026**

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Alison Llewellyn and Katie Hewson
Stephenson Harwood
Richard Jeens and William Doyle
Slaughter and May
Mark Read
TransUnion
Gary Brooks
Data Protected
Annabel Gillham and Michelle Luo
Morrison Foerster

PUBLISHED BY
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* United Kingdom Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.
Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2047-1479

comment

PL&B's 40th anniversary year coincides with new DP regime

As *PL&B* celebrates its 40th year in business, we are pleased to announce our 39th Annual International Conference, including confirmed speakers from the ICO and Data Protection Authorities from Ireland, Kenya, Singapore and the European Data Protection Board (p.17).

Part of the conference programme in Cambridge will discuss the changes that the Data (Use and Access) Act brings to organisations. Now that most of the remaining data protection provisions of the Act have come into force, the onus is on ensuring compliance and making the most of the simplifications (p.11). This also applies to SARs – our comprehensive guidance on how to manage SARs is important reading for everyone (p.18).

One remaining part of DUAA still to enter into force is the requirement for organisations to have a complaints procedure. While this will commence on 19 June 2026, the ICO has already issued guidance (p.10). This includes advice for organisations on how to manage their complaint processes but also confirms the ICO's stance: it will prioritise cases that cause significant harm, affect large numbers of people, raise issues of wider public interest, or relate to vulnerable individuals.

A data breach can have a significant psychological effect on an individual (p.8). As our correspondent says, a breach triggers a cascade of emotions, fear, anger, and helplessness, which can persist long after the technical incident is resolved.

In its enforcement, the ICO is now placing a significant focus on cyber and data security failings. Our correspondents offer tips in this edition on how to handle an ICO investigation and look into 2026 trends on p.1.

This spring, look out for further announcements on the Privacy and Electronic Communications Regulations (PECR) as the ICO is committed to reviewing PECR consent requirements for advertising (p.22).

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you wish to contribute to *PL&B UK Report*? Please contact Laura Linkomies, Editor (tel: +44 (0)20 8868 9200 or email: laura@privacylaws.com) to discuss your idea, or offer to be interviewed about your organisation's data protection/Freedom of Information work.

Enforcement... from p.1

powers under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

The draft Guidance is a comprehensive document that aims to bring greater clarity, transparency, and predictability to the ICO's enforcement processes. Once finalised, the Guidance will replace the ICO's 2018 Regulatory Action Policy (Regulatory Action Policy), providing significantly more clarity and detail on each stage of an ICO investigation and the exercise of its statutory powers.

The Guidance reflects not only the ICO's evolving approach to its investigatory and enforcement capabilities but also incorporates important guidance on its new powers introduced by the Data (Use and Access) Act 2025 (DUAA), the data protection aspects of which came into force on 5 February 2026.

Among the most notable changes, the Guidance covers the ICO's expanded ability to issue assessment notices requiring the preparation of reports by "approved persons" and to require individuals to attend interviews and answer questions; both tools designed to strengthen oversight and assess controllers' and processors' compliance with the UK data protection regime.

With the consultation period having closed on 23 January 2026, we are now awaiting the outcome of the consultation and the final version of the Guidance. In this article, we take an in-depth look at the draft Guidance. We highlight key takeaways, practical points that are likely to assist companies, any remaining uncertainties, and what organisations should be monitoring as the ICO adapts to its enhanced investigative and enforcement capabilities.

Overview and key takeaways

The Guidance is a significant evolution from the Regulatory Action Policy and is a step forward in demystifying the ICO's enforcement approach. It is more detailed, transparent, and focused on procedure. The Guidance sets out a structured process through the lifecycle of an ICO investigation into a potential breach of data protection legislation, from the decision to open a case to the investigation, the final outcome and subsequent rights of appeal.

The Guidance is organised into the following sections:

- How the ICO decides whether to open an investigation.
- What to expect during an investigation.
- The ICO's information gathering powers.
- Limits on the ICO's investigatory powers.
- Decision-making and outcomes.
- Processes for warnings, reprimands, enforcement notices, and penalties.
- Settlement procedures.
- Rights of appeal.

The structured approach and increased transparency should help organisations prepare for and manage ICO investigations more effectively, which in turn should reduce the risk of procedural missteps and unexpected events.

We consider some of the key changes in more detail below.

Criteria for opening an investigation

The Guidance emphasises prioritisation, with the ICO stressing the importance of acting proportionately and using its resources efficiently. It confirms that not every complaint or breach will lead to a formal investigation. Instead, it will focus on cases with serious actual or potential harm to individuals. The Guidance details the wider strategic and policy factors the ICO will consider, including the scale of impact, resource implications, alignment with ICO priorities, the extent to which opening an investigation would support economic growth and the need to deter similar conduct by others.

This risk-based approach is likely to be welcomed by organisations, as it suggests that minor or technical breaches are less likely to attract the ICO's full enforcement approach, provided they are addressed appropriately. That said, the weighting of the above factors is not specified, and the "strategic objectives" referenced are not always clear. This approach allows subjectivity into the ICO's approach to prioritisation which makes it more challenging to predict which cases will be pursued.

Applying this to recent topics by way of illustration, it was with notable urgency that the ICO issued a public statement regarding its formal investigation into X's Grok artificial intelligence tool following widespread public concern and Ofcom's announcement of its own investigation. In contrast, the ICO decided not to investigate the Ministry of Defence's (MoD) Afghan data breach, opting instead to oversee the MoD's internal review, primarily due to claims of limited resources, the MoD's high-security classification of the data, and a "super-injunction" restricting information. The ICO contended that a separate investigation would not have added value, despite criticism that this decision reflected a reluctance to hold government agencies accountable and was an example of the ICO's shift away from taking enforcement action.

Building these factors for consideration explicitly into the Guidance demonstrates the ICO's commitment to transparency in its decision-making process, while preserving continued flexibility and discretion for the regulator.

Information gathering

An important element in the Guidance is the clarification that, alongside its formal information gathering powers under the DPA 2018, the ICO may request that a controller or processor provides information voluntarily, specifying deadlines and formats for responses. The Guidance encourages early engagement and voluntary cooperation, with the ICO confirming that it may accept written assurances or undertakings to remedy issues without opening a formal investigation.

The Guidance indicates that voluntary cooperation with the ICO may be considered a mitigating factor when deciding whether to issue a fine and its level. However, this is in addition to an organisation's ordinary duty of cooperation required by law (which would not constitute a mitigating factor). It is not clear from the Guidance what would distinguish ordinary from mitigative cooperation. Conversely, persistent and repeated behaviour that delays regulatory action may be treated as an aggravating factor when considering whether to impose a fine.

New powers granted under the DUAA

A key focus of the updated Guidance is the new powers introduced by the DUAA.

Power to require production of documents: Amendments to the UK GDPR made by the DUAA clarify that the ICO, under its power to issue an information notice, can require the production of specific documents, not just specific information.

The explanatory notes to the DUAA describe this as a clarification of the ICO's existing powers, and this is not a new concept introduced by the Guidance. Nevertheless, the clarification could lead the regulator to change its approach in practice, with the ICO more empowered to require documents to be produced in the course of its investigations, which it has not typically done up to now.

This poses a potential risk to organisations, as the regulator may not have the full context for particular documents provided. Organisations should ideally ensure, when providing a document, that it is accompanied by appropriate explanation. The enhanced power may also present a greater compliance burden for organisations that must locate and provide the specific documents requested, checking also that legally privileged information is not disclosed.

Power to require preparation of a report: The ICO can now mandate the production of a report by an "approved person". This power can be seen as similar to the "skilled person" regime in a financial services regulatory context. The Controller must bear the cost of producing the report and the ICO can specify the subject matter of the report, the form and manner in which it must be prepared, and the date by which it must be provided.

The Guidance sets out in detail its decision-making process for the exercise of this power, but does not give a clear indication of how often the ICO anticipates it will use this power, nor how it could influence enforcement action. One scenario in which it is likely that the ICO will make use of this power is in the context of personal data breaches, for example, to require a report into the adequacy of security measures in place at the time of a breach.

Power to issue interview notices: The ICO's significant new investigatory power under the DUAA allows it to issue interview notices where the ICO suspects a failure to comply with the UK GDPR or the DPA 2018, or that a relevant criminal offence under the DPA 2018 has been committed. Interview notices may be issued to:

- the controller or processor;
- an individual employed by, or otherwise working for, the controller or processor (or was at any time); and
- an individual involved in the management or control of the controller or processor (or was at any time).

This is notably broad in scope, particularly given that interview notices may be issued to anyone in the organisation, not just DPOs, but also to current and former employees, with no time limits as to how long ago a person may have been employed by the relevant organisation. Organisations should ensure that their staff training covers how to respond if such an interview request is made.

Individuals can appeal against an interview notice and, ordinarily, such a notice will not be able to require an individual to attend and be interviewed at a time before the expiry of the appeal period. However, in urgent cases, the ICO can require attendance sooner, and failure to attend could result in a fine.

Formal settlement process

A key change in the Guidance is the introduction by the ICO of a formal settlement process. This includes a streamlined and more transparent procedure with discounts on penalties for early resolution. The Guidance offers detailed indications of when the ICO might consider accepting a settlement offer, requiring that the entity under investigation must admit the nature, scope and duration of a breach in order for settlement to be possible, and setting out how the process of settlement would operate in practice.

The Regulatory Action Policy only made passing reference to settlement, so the Guidance in comparison is far more granular. In particular, it details a new structured settlement procedure that effectively provides an incentive to organisations to be proactive and transparent when issues arise, potentially reducing the financial and reputational impact of enforcement. The Guidance sets out a sliding scale of discounts, to be determined on a case-by-case basis, for entering into settlement discussions and concluding a case, up to the following maximum amounts:

DISCOUNTS

Maximum discount	Settlement point
40%	Before notice of intent is issued.
30%	After issuing notice of intent but before receipt of written representations.
20%	After issuing notice of intent and after receipt of written representations.

The Guidance makes clear that the above approach is not fixed and the ICO retains significant autonomy to bring settlement discussions to an end or reduce the available discount. It also confirms that an organisation's engagement (or otherwise) in settlement discussions is not considered as an aggravating or mitigating factor when deciding whether to impose a penalty or determine the amount of any fine.

Any grey areas?

While the Guidance is a major step forward, several grey areas and potential challenges remain.

Non-binding guidance: The ICO repeatedly emphasises that the Guidance is not binding and that it may depart from its stated approach where there are "good reasons to do so in the specific circumstances of a case." This preserves the ICO's wide discretion to use its powers and conduct its investigative and enforcement processes in a flexible way. While this flexibility is understandable, it does introduce some uncertainty for organisations seeking predictability.

Early engagement and cooperation: Organisations should be prepared to respond promptly and comprehensively to ICO enquiries,

whether voluntary or formal. Delays, incomplete responses, or lack of cooperation could be treated as aggravating factors and could increase penalties or change the regulator's approach to investigation.

Overlap with other regulators: The Guidance acknowledges that other regulators (e.g. the FCA, Ofcom, or the CMA) may be better placed to act in some cases. However, the process for coordination and referral is not fully spelled out, raising questions about parallel investigations and regulatory overlap.

Discretionary settlement procedure: The new settlement procedure is a welcome innovation, but some aspects remain unclear. The criteria for eligibility and the calculation of discounts are not fully detailed, and the process is entirely discretionary (i.e. an organisation cannot make the decision to enter into settlement discussions). The window for maximum benefit is very narrow, so organisations should assess the risks and benefits of settlement as soon as possible after an investigation is opened and before a notice of intent is issued.

Open settlement discussions: Settlement discussions are "open" meaning information shared can be used in later proceedings if settlement fails. This absence of a 'without prejudice' framework also requires careful consideration and could deter some organisations from taking this route.

What comes next?

The Guidance represents a major step forward in clarifying the regulator's approach to investigations and enforcement. For organisations required to comply with UK data protection legislation, the Guidance offers greater transparency, predictability, and opportunities for early engagement and resolution. However, significant discretion remains with the ICO, and organisations should not assume that the Guidance will be applied rigidly in every case.

Overall, the Guidance highlights the importance of cooperation, proactive compliance, early engagement, and strategic decision-making when under investigation by the ICO.

As the UK data protection landscape, and the risk environment, continues to evolve, and the ICO settles into its enhanced investigation powers, organisations should monitor developments closely and ensure that their policies, procedures, and response plans remain fit for purpose.

AUTHORS

Alison Llewellyn, Senior Knowledge Lawyer, and Katie Hewson, Partner, Stephenson Harwood.
Emails:
alison.llewellyn@stephensonharwood.com
katie.hewson@stephensonharwood.com

Join the Privacy Laws & Business community

The *PL&B United Kingdom Report*, published six times a year, covers the Data (Use and Access) Act 2025, the UK GDPR, the Data Protection Act 2018, Privacy and Electronic Communications Regulations 2003 and related legislation.

PL&B's United Kingdom Report will help you to:

Stay informed of data protection legislative developments.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Learn about future government/ICO plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to privacy and data protection law issues and tech developments that will affect your compliance and your reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
Search for the most relevant content from all *PL&B* publications.

3. Electronic Versions
We will email you the PDF edition which you can also access in online format via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments.

6. Back Issues
Access all *PL&B UK Report* back issues.

7. Events Documentation
Access *PL&B* events documentation, except for the Annual International Conferences in July, Cambridge.

8. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

9. Free place at a *PL&B* event
A free place at a *PL&B* organised event when booked a specified number of days in advance. Excludes the Annual Conference. More than one free place with Multiple and Enterprise subscriptions.

privacylaws.com/reports

"*Privacy Laws & Business* not only acts as a useful and comprehensive summary of recent key developments in our area of specialism, but also provides excellent, in-depth insight and analysis to drive thought leadership. It's an invaluable source of information."

Emma Erskine-Fox, Partner, TLT LLP

International Report

Privacy Laws & Business also publishes *PL&B International Report*, the world's longest running international privacy laws publication, now in its 40th year. Comprehensive global news, currently on 180+ countries, legal analysis, management guidance and corporate case studies on privacy and data protection, written by expert contributors

Read in more than 50 countries by regulators, managers, lawyers, and academics.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.