New Act enhances enforcement and investigatory powers

The Data (Use and Access) Act 2025: What do organisations need to know?

By **Katie Hewson**, **Joanne Elieli** and **Alison Llewellyn** of Stephenson Harwood.

The UK's data protection landscape is undergoing its first significant transformation since Brexit reshaped the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) and introduced the UK GDPR. The Data (Use and Access) Act 2025 (DUAA), which received Royal Assent on 19 June 2025, introduces key changes to the current structure, powers and enforcement capabilities of the UK's data protection regulator.

When the relevant provisions come into force via secondary legislation – the bulk of which are currently expected to be phased in around December 2025 – the Information Commissioner's Office (ICO) will be replaced by a new body, the Information Commission (IC), with a modernised corporate structure and an enhanced suite of investigatory and enforcement powers.

Amongst the most notable will be the IC's ability to compel individuals to attend interviews to be questioned as part of the IC's investigations, and the IC's authority to require organisations to prepare, or commission the preparation of, technical reports by approved experts.

These developments mark a shift in the IC's regulatory oversight that has generated much debate. The ICO's strategic approach won't change in the short term, and the upcoming changes should not have a significant impact on the burden of compliance. In particular, the ICO has been keen to emphasise that its enhanced regulatory powers aren't focused on imposing fines. Rather, they are intended to facilitate the provision of upfront support and encourage a collaborative approach to identifying and addressing compliance issues to help avoid enforcement action. However, the changes will demand careful consideration by organisations in order to remain well-prepared in the event of any enforcement action by the IC.

This article explores the key changes, the rationale behind them, and practical steps that organisations should take to prepare for these new regulatory developments.

Information Commission: Structure and independence

The changes introduced by the DUAA to the structure of the ICO, by replacing the ICO's "corporation sole" model with a full corporate structure, will bring the UK's data protection regulator in line with other major UK regulators, such as Ofcom and the Financial Conduct Authority.

The new IC will be led by a Chair, Chief Executive, and a Board of between three and 14 non-executive and executive members with shared decision-making responsibilities. The Secretary of State will determine the precise number of board members and is required, as far as practicable, to ensure that non-executive directors outnumber executive directors.[1] This approach is designed to enhance overall diversity and resilience when it comes to decision-making and aims to reinforce the independence and accountability of the regulator, addressing previous criticisms that the ICO's structure was outdated and less robust than those of its regulatory peers.

> Staff at all levels should be made aware of the upcoming powers of the IC.

Interestingly, the DUAA omits a controversial provision from the previous Data Protection and Digital Information Bill that would have allowed the UK Government to set strategic priorities for the IC. This omission was widely seen as a move to safeguard the IC's independence and to preserve the UK's data adequacy status with the EU, a key priority of the current government; a move which has been successful, with the European Commission launching its process to adopt new adequacy decisions under the GDPR and Law Enforcement Directive in July 2025.

John Edwards, the current Information Commissioner, retains his title and will serve as the first Chair of the IC, continuing his term until January 2027. Future chairs will be appointed through an open competition, with a maximum term of seven years and a prohibition on reappointment. Paul Arnold has been appointed the first CEO of the IC. The IC was established, albeit initially without functions, with effect from 20 August 2025.

Enhanced investigatory and enforcement powers

Right to require documents: With effect from 19 August 2025, the DUAA enhances the ICO's investigatory powers by clarifying that it can require the production of specific documents, as well as specific information, under its power to issue an information notice. While the ICO previously had the ability to request information, this expansion makes it explicit that the regulator can also require the provision of specified documents, including emails, internal reports, and other records.

This clarification is intended to enable the IC to conduct more thorough and effective investigations by ensuring that it has access to the documentary evidence needed to assess compliance. However, it risks increasing the compliance burden on organisations, which will need to be able to

locate, review, and provide relevant documents promptly. The change, however, may result in a reduced ability for organisations to contextualise information being disclosed to the IC and could have the effect of more information being disclosed than was specifically sought by the IC, e.g. where the information requested forms part of a wider document. Organisations should therefore ensure that any documents provided to the regulator are accompanied – where possible – by appropriate explanations and/or narratives to provide context and avoid misinterpretation.

Power to compel witness interviews: One of the most significant new powers to be conferred on the IC is the ability to issue "interview notices." For the first time, the regulator will be able to require individuals to attend interviews and answer questions in the context of investigations into potential breaches of the UK GDPR or the DPA. This power is available where the IC suspects non-compliance with data protection law and/or the commission of a relevant criminal offence.

The scope of this power is notably broad. Interview notices may be issued to:

- an individual in their capacity as controller or processor;
- any individual currently or previously employed by the controller or processor; and
- any individual currently or previously "concerned in the management or control" of the controller or processor.

For organisations, the new interview power raises important considerations, particularly as there is no specified limitation as to the IC's powers to compel former employees or managers to attend interviews and participate in an investigation. The breadth of this power is unprecedented in the UK data protection context and brings the IC's investigatory toolkit closer to that of other major regulators.

The DUAA does include certain safeguards. Interview notices cannot be issued where Parliamentary or legal privilege applies, and individuals cannot be compelled to answer questions that would incriminate them — except in relation to offences under the DPA, which are expressly excluded from this protection. This means that individuals can be required to answer questions that may self-incriminate in respect of DPA offences.

Non-compliance with an interview notice, such as failing to attend an interview, will be an offence. It will also be an offence knowingly or recklessly to make a materially false statement during an interview, and the IC will have the power to impose a penalty notice, with significant fining powers aligned to those currently held by the ICO. Individuals have the right to appeal against an interview notice, and in most cases, the notice cannot require attendance before the expiry of the appeal period, unless the IC deems the matter urgent.

As a relatively extensive list of individuals could potentially be called to an IC interview in future, organisations would be well-advised to prepare policies (if not already covered by existing ones) and train relevant individuals in advance on who to speak to and what to expect in the event of receiving an interview notice; and to provide support (and potentially independent legal advice) if an employee or former employee is called to interview.

Power to require technical reports: Another key development will be the IC's power to require organisations to commission and provide technical reports prepared by approved experts. This builds on the existing assessment notice regime, which allows the regulator to require organisations to undergo audits or assessments of their data protection practices.

Under the new regime, when the IC issues an assessment notice, it may require the recipient to instruct an "approved person" to prepare a report on a specified subject. The IC can dictate the content, form, and deadline for the report, and the organisation must bear the cost of its preparation. The organisation may nominate a person to prepare the report, but the IC must approve the nominee and may reject them if they are deemed unsuitable. If the organisation fails to nominate an approved person within the specified timeframe, the IC can appoint someone of its own choosing.

This power is likely to be used in the context of personal data breaches, where the IC requires a report on the adequacy of the security measures in place at the time of the incident. However, the scope of the power is not limited to security breaches and could extend to any aspect of data protection compliance, such as data minimisation, retention practices, or data sharing arrangements.

Importantly, reports prepared under this regime do not benefit from legal privilege in relation to disclosure to the IC. This means that the contents of a report could be used as evidence in enforcement proceedings or even in subsequent litigation brought by data subjects or other third parties. Organisations should be mindful that any findings of non-compliance or inadequacy set out in such a report could be relied upon by claimants seeking to establish liability.

The requirement to commission and pay for potentially costly technical reports also represents a significant new compliance burden, particularly for smaller organisations or those with limited resources, and a shift in the cost of data breach incident analysis from the regulator onto the affected organisation. It is essential that organisations put in place robust mechanisms for managing the preparation of such reports, including careful selection of experts, thorough review of draft reports, and clear documentation of the context and rationale for any findings or recommendations.

Longer timelines for penalty notices: The DUAA extends the period within which the IC can issue a final penalty notice following a notice of intent. Previously, the regulator was required to issue the final notice within six months of the notice of intent. When the relevant provisions come into force, this period can be extended if it is not reasonably practicable to meet the six-month deadline, allowing the IC more time to investigate complex cases and consider representations from the parties involved.

While this change is intended to improve the quality and thoroughness of investigations, it may also result in longer and more resource-intensive enforcement processes for organisations under investigation.

Increased enforcement powers for PECR breaches: The DUAA brings

the penalty regime for breaches of the Privacy and Electronic Communications Regulations (PECR) in line with those under the UK GDPR and DPA. The maximum fines for certain PECR breaches, such as unlawful direct marketing, will increase from the current cap of £500,000 to £17.5 million or 4% of global annual turnover, whichever is higher. For other PECR breaches, the maximum penalty will be £8.7 million or 2% of global annual turnover.

The IC's powers to issue information, assessment, interview, enforcement, and penalty notices in relation to PECR breaches will also be aligned with those under the UK GDPR and DPA. This reflects the regulator's continued focus on compliance with cookies rules and the AdTech sector, and underscores the importance for organisations operating in these areas to prioritise compliance and prepare for more robust enforcement action.

How to prepare

The majority of the substantive amendments to data protection law under the DUAA, including the IC's new powers, are not yet in force. The ICO has expressed a desire to implement provisions swiftly, but recognises that additional steps will be required for the provisions to be a success, such as allowing time for ICO guidance to be prepared, consulted upon, and implemented.

The ICO is required to produce and publish guidance on the use of its new powers, including the factors to be considered when deciding to issue an interview notice, and has confirmed that it will consult publicly on the preparation of such guidance nearer to the commencement of the relevant DUAA provisions. However, an indicative timeframe for guidance on the ICO's new powers has not yet been provided on the ICO's new dedicated *planned guidance page*,[2] which details the nature, scope and timeline for publication of new and updated guidance, including to reflect the DUAA.

In the meantime, organisations should take proactive steps now to ensure they are prepared to respond effectively to the upcoming changes.

1. Legal and regulatory risk assessment: Organisations should conduct a risk assessment to identify areas of potential non-compliance with data protection legislation and take steps to address any gaps. This may include engaging external legal or compliance experts to review practices and provide guidance on best practices for compliance with the UK GDPR and DPA.

2. Review and update policies and procedures: Organisations should consider reviewing and updating their internal policies and procedures for responding to regulatory investigations. This may include ensuring that there are clear internal protocols for how to respond to interview notices, information and document requests, requirements to commission technical reports, and how to manage associated legal and reputational risks.

3. Document management and record-keeping: Organisations should reflect on the importance of upholding the UK GDPR's accountability principle. Robust document management and record-keeping systems are essential to ensure that organisations can locate and provide relevant documents promptly in response to regulatory requests. Organisations should also ensure, where possible, that any documents provided to the regulator are accompanied by appropriate explanations to provide context and avoid misinterpretation.

4. Employment contracts and post-termination provisions: Given the IC's power to compel interviews with former employees and managers, organisations should consider a review of employment contracts and post-termination provisions to ensure that former staff are aware of their potential obligations, and the organisation can facilitate cooperation with the regulator if so required.

5. Managing technical reports: Organisations may wish to identify and maintain relationships with experts in their sector who could be called upon to prepare technical reports if required by the IC. Internal processes should be established to manage the commissioning, review, and submission of such reports, including ensuring that findings are accurate, balanced, and provide appropriate context.

6. Training and awareness: Staff at all levels should be made aware of the upcoming powers of the IC and the organisation's obligations under the DUAA once the relevant provisions come into effect. Organisations may consider providing additional training to key personnel, including HR, legal, compliance, and IT teams, to ensure that they understand how to respond to regulatory requests and investigations, including supporting individuals called to interview.

Conclusion

The DUAA marks a significant evolution in the UK's data protection regulatory framework. The creation of the IC and the expansion of its investigatory and enforcement powers indicates the potential for a more robust and proactive approach to overseeing data protection compliance.

By taking proactive steps now to review and update policies, procedures, and contracts, and by fostering a culture of compliance and accountability, organisations should be able to position themselves to respond effectively to the new powers of the IC, and minimise the risks associated with non-compliance. As the relevant provisions of the DUAA come into force and the IC begins to exercise its new powers, organisations should remain vigilant, informed, and be prepared to engage constructively and cooperatively with the regulator.

AUTHORS

Katie Hewson and Joanne Elieli are both Partners at Stephenson Harwood. Alison Llewellyn is a Senior Knowledge Lawyer at the same firm.
Emails:
Katie.Hewson@stephensonharwood.com
Joanne.Elieli@stephensonharwood.com
Alison.Llewellyn@stephensonharwood.com

REFERENCES

1 In June, the Department for Science, Innovation and Technology started the recruitment process for seven non-executive members. It is expected that the appointments will be made by the end of 2025. See apply-for-public-appointment.service.gov.uk/roles/8609
2 ico.org.uk/about-the-ico/what-we-do/our-plans-for-new-and-updated-guidance/

ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

DUAA data protection aspects in force by the end of this year

Laura Linkomies reports on the steps DSIT and the ICO are taking to implement the law, and issue guidance.

The Data (Use and Access) Act (DUAA) amends, but does not replace, the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA) and the Privacy and Electronic Communications Regulations (PECR).

The government has now issued commencement regulations. While some of the provisions have already entered into force, the data protection part of the Act will be mostly brought into force approximately six

Continued on p.3

ICO fines 23andMe £2.31m – what have we learned?

Taylor Wessing's **Mike Vallance** looks at the ICO's final conclusions on the DNA testing site 23andMe data breach and at key takeaways.

The 23andMe data breach has caught the attention of the privacy community as a clear and stark reminder of the damage that can be caused by a data breach. On 17 June 2025, the UK Information Commissioner's Office (ICO) announced a revised fine of £2.31 million to be imposed on the prominent consumer genetics company[1] following a data breach that exposed sensitive genetic and health information of

Continued on p.5

Future *PL&B* Events

Maximising opportunities from the Data (Use and Access) Act 2025
1 October 2025, Host: Linklaters, London
www.privacylaws.com/UK2025

Minding the (US-European) Privacy Gap
4 November 2025, Host: Latham & Watkins, London
www.privacylaws.com/USA2025

Meet the *PL&B UK Report* Correspondents
3 December 2025, Host: Stephenson Harwood, London
www.privacylaws.com/correspondents2025

Issue 141 **SEPTEMBER 2025**

See the publisher's blog at privacylaws.com/blog2025sep

UNITED KINGDOM
report

ISSUE NO 141 **SEPTEMBER 2025**

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
Nicola Fulford and Robert Fett
Hogan Lovells

Mike Vallance
Taylor Wessing

Katie Hewson, Joanne Elieli and Alison Llewellyn
Stephenson Harwood

Geraldine Scali and Anna Blest
Bryan Cave Leighton Paisner LLP

Nel Anna Krzeslowska
PL&B Correspondent

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

ICO on the fast track

The new Data Use and Access Act 2025 (DUAA) may not be radically different from the Data Protection Act 2018, yet it requires the ICO to conduct a full review of its existing guidance as the majority of the data protection provisions of the Act are expected to be in force just before the end of 2025. Updates are expected in a rapid fashion – ICO consultations are already underway on legitimate interests and complaints procedures (p.4). In the summer, the regulator was also seeking views on its data transfer guidance under the UK GDPR. This is a hot potato considering for example the recent Ireland DPC fine on TikTok's transfers to China. When reading the response by law firm Hogan Lovells, I feel that many may join them in spirit in asking the ICO to adopt and promote a more streamlined approach to transfer risk assessments, especially when the data in question is not sensitive.

The regulator is now working on updating guidance for automated profiling tools to help users who use them to meet their obligations under the Online Safety Act 2023 (p.16). Data Subject Access Request (DSAR) guidance will also be looked at in light of the DUAA – although much of it is already adopted by the ICO in its day-to-day work (p.13). However, organisations may wish to review their DSAR policies now to prepare for the new data subjects' right of complaint.

The DUAA will enhance the ICO's enforcement powers (p.10), and especially under PECR, where fines for breaches increase to UK GDPR levels – up to £17.5m or 4% of annual worldwide turnover (p.8).

I look forward to our half-day conference on 1 October to hear more about work on DUAA implementation (see p.15). Before that, I am delighted to be able to attend the Global Privacy Assembly in South Korea later this month, and to report for our sister publication, *PL&B International Report*.

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.linkomies@privacylaws.com) to discuss your idea, or offer to be interviewed about your organisation's data protection/Freedom of Information work.

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

"Fantastic documents which provide a useful snapshot of the data protection landscape all in one place that can be easily digested around your busy working day. The split between International and UK allows you to focus on areas of interest as you require."

Angela Parkin, Group Director of Data Protection, Equiniti

International Report

Privacy Laws & Business also publishes *PL&B International Report*, the world's longest running international privacy laws publication, now in its 39th 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.