Are we moving towards a more permissive UK framework for life sciences research data?

Further processing for research purposes is presumed compatible with the original purpose of data collection, the ICO says. By **Sarah O'Brien**, **Bobbie Bickerton** and **Alison Llewellyn** of Stephenson Harwood.

Organisations, particularly those in the life sciences sector, should take note of the ICO's draft updates to its guidance on the Research, Archiving and Statistics (RAS) provisions[1] (the Guidance) under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). The RAS provisions themselves are not new. What is new is the way the Guidance responds to amendments introduced by the Data (Use and Access) Act 2025 (DUA Act 2025) and reflects the ICO's updated expectations on how personal data can be used for research purposes under UK law.

The DUA Act 2025 amends the UK GDPR to clarify and, in some respects, broaden the framework for the use of personal data in scientific research and other research-related purposes. The RAS provisions cover four types of research-related purposes: archiving in the public interest; scientific research; historical research; and statistical purposes.

Aimed at data protection officers and those with data protection responsibilities in organisations undertaking research, archiving or statistical processing, the Guidance explains how the RAS provisions work, the exemptions available, and how those provisions interact with the data protection principles, lawful bases and wider compliance obligations under UK data protection law.

UK data protection law has long recognised the importance of scientific and historical research and technological development to society. The DUA Act 2025 amendments – reflected in the updated Guidance – are designed to ensure that data protection requirements enable, rather than hinder, technological innovation and the advancement of knowledge, particularly in the healthcare and technology sectors.

The Guidance is timely: it comes at a moment when the use of large-scale datasets – including for AI-enabled research and machine learning – is attracting growing regulatory and commercial attention across the UK and the EU, as both jurisdictions refine their approaches to data-driven research.

Consultation

The ICO consultation on the Guidance opened on 27 February 2026.[2]

The ICO has specifically invited feedback on its position regarding the new disproportionate effort exemption (introduced by section 77 of the DUA Act 2025) under which organisations are no longer required to inform data subjects about the re-use of previously collected data where such re-use is for research purposes and providing such information would involve disproportionate effort. This is one of the clearest genuinely new DUA Act 2025 changes discussed in the Guidance.

What does the Guidance say?

Scope of research-related processing: The DUA Act 2025 defines scientific research broadly as: "processing for the purposes of any research that can reasonably be described as scientific, whether publicly or privately funded and whether carried out as a commercial or non-commercial activity". Brought into effect by secondary legislation on 5 February 2026, this aligns the substantive provisions of the UK GDPR with existing recitals and regulatory guidance. A new Article 4(3) UK GDPR confirms that, provided the processing can reasonably be described as scientific, this includes technological development and demonstration, fundamental research, applied research, and public health studies in the public interest. The Guidance underscores this broad assessment by expressly identifying real-world evidence research and secondary use of clinical trial data as falling within scope – a particularly important point for the life-sciences sector – and clarifies that scientific research can be carried out by public sector bodies, commercial organisations, charitable organisations, and independent researchers.

What the Guidance adds, in practical terms, is a four-criteria framework to help organisations determine whether their processing qualifies as scientific research:

- **Scientific objective**. To qualify as scientific research, the ICO expects organisations to demonstrate that their work aims to make a meaningful improvement in science or technology, including public health, that benefits the entire field, not just the organisation conducting the research.
- **Scientific method**. The work must be well planned, documented, and systematically carried out in accordance with ethical standards, with a methodology consistent with accepted standards in the relevant scientific or technical field.
- **Uncertainty**. There must be genuine scientific or technical uncertainty at the outset of the research - commercial uncertainty alone is not sufficient.
- **Transferability**. The research must produce results or knowledge that are capable of wider application, for example, by being built upon by others, disseminated within a research community, or incorporated into broader scientific

understanding. Publication is not strictly required, but the outputs must have applicability beyond the organisation conducting the research.

Requirements and safeguards

Article 84B UK GDPR, introduced by the DUA Act 2025, now provides that personal data may only be processed for RAS purposes where the processing consists of data collection, anonymisation, or processing without which the RAS purposes cannot be fulfilled. Article 84C UK GDPR details the safeguards required: the processing must not be likely to cause substantial damage or substantial distress; it must not be used to inform measures or decisions about the individuals concerned (except in approved medical research); and there must be technical and organisational measures to ensure respect for data minimisation, including, where possible, pseudonymisation or anonymisation.

The Guidance sets out the specific safeguards the ICO considers appropriate to satisfy these requirements, including: taking a data protection by design and default approach; implementing appropriate security measures; carrying out data protection impact assessments where necessary; appointing a data protection officer where required; providing appropriate staff training; and using privacy-enhancing technologies such as Trusted Research Environments. The ICO also endorses the use of accountability frameworks – in particular, the Five Safes Framework[3] – as a means of demonstrating compliance. These are not statutory requirements, but represent the ICO's view of good practice and are likely to inform its approach to enforcement.

Impact on data protection principles and lawful bases

The Guidance explains how the RAS provisions interact with two key data protection principles: purpose limitation and storage limitation. Article 8A UK GDPR expands on the purpose limitation principle by deeming further processing for RAS purposes compatible with the original purpose, provided appropriate safeguards are in place; no separate compatibility assessment is required. The storage limitation principle, in turn, permits organisations to retain personal data indefinitely where it is processed solely for RAS purposes with appropriate safeguards.

The Guidance confirms that there is no specific lawful basis for research-related processing. Organisations are most likely to rely on either the legitimate interests or public task legal bases, depending on the type of organisation and context. The ICO makes the important practical point that consent to participate in a research study is distinct from consent as a UK GDPR lawful basis. Indeed, the Guidance notes that in most cases, consent is not the most appropriate lawful basis for research processing, because of the difficulties that arise when participants seek to withdraw consent.

Where personal data was originally collected on the basis of consent for one purpose, the general position is that fresh consent must be obtained before reusing it for a different purpose, including a research purpose. The DUA Act 2025 updates to the UK GDPR, however, recognise "broad consent" to research where the specific research purposes cannot be fully identified at the time of collection, provided ethical standards are maintained and individuals are given the opportunity to consent to specific areas of research where possible. This is particularly significant for biobanks and patient registries, where the full scope of future research uses cannot be anticipated at the point of data collection.

Exemptions from data subjects' rights

The Guidance addresses the exceptions and exemptions from data subjects' rights that apply to research-related processing, covering the rights to be informed, access, rectification, erasure, restriction of processing, data portability, and objection, including the disproportionate effort exemption noted above. Some are built-in exceptions in the UK GDPR itself (notably Article 17(3)(d) for the right to erasure); others are separate exemptions in Schedule 2 paragraphs 27 and 28 of the DPA 2018. The Guidance is clear that organisations must not rely on these exceptions or exemptions in a blanket fashion: each must be applied on a case-by-case basis and only where complying with the relevant right would prevent or seriously impair the achievement of the research purposes.

Disproportionate effort is not entirely new in this context. Pre-DUA Act 2025, the UK GDPR already provided an exception to the obligation to inform data subjects where personal data had not been obtained directly from the data subject and providing information would involve disproportionate effort. The exemption has now been extended to scenarios where the personal data was originally collected directly from the data subject specifically for research purposes. This is a meaningful expansion, enabling organisations to re-purpose data they themselves collected without having to provide fresh privacy information to each data subject, taking into account appropriate safeguards.

This exception to the right to be informed is of direct practical relevance to life sciences organisations that routinely seek to re-purpose clinical, real-world, or registry data for secondary research, as it provides a lawful mechanism to proceed without individual notification where the scale or nature of the dataset makes direct communication impracticable. When assessing disproportionate effort, factors such as the number of individuals affected, the age of the information, and safeguards adopted should be considered. Even where disproportionate effort is established, the ICO expects organisations to publish the relevant privacy information and carry out a data protection impact assessment.

Impact on life sciences organisations

First, the broad UK definition of scientific research – expressly including commercially funded research, technological development, applied research, public health studies, real-world evidence research and secondary use of clinical trial data – provides a stronger and clearer foundation for pharmaceutical companies, Contract Research Organisations (CROs) and health technology businesses to rely on the scientific research limb of the RAS provisions. The ICO's new four-factor test offers a structured framework for

self-assessment, though careful documentation will be required.

Second, the clarification that further processing for research purposes is presumed compatible with the original purpose of data collection will provide life sciences organisations with the opportunity to re-purpose clinical trial data, patient registry data, or real-world evidence datasets for secondary research. Removing the need for a separate compatibility assessment, provided appropriate safeguards are in place, should reduce the compliance burden associated with such activities.

Third, the ICO's express statement that consent is not, in most cases, the most appropriate lawful basis, reinforces the industry-standard position taken by clinical trial sponsors and CROs to rely instead on legitimate interests rather than navigating the distinction between ethical/clinical trial consent and consent as a UK GDPR lawful basis. The ICO acknowledges that carrying out research, with appropriate safeguards in place, effectively addresses the issues a legitimate interests assessment would cover.

Finally, the exemptions from data subjects' rights, while valuable, remain subject to careful and documented case-by-case assessment. Notwithstanding the disproportionate-effort route for information obligations, the broader point maintained in the Guidance is that blanket reliance on rights exemptions is not acceptable. Organisations must inform individuals when their rights are being restricted, including their right to complain. Robust internal processes for handling rights requests in the context of ongoing research will be essential.

Differences from the EU approach

The European Data Protection Board (EDPB) adopted draft Guidelines 1/2026 on the processing of personal data for scientific research purposes on 15 April 2026, which were open for public consultation until 25 June 2026.[4] The parallel development of both UK and EU guidance provides a useful basis for comparison.

The most notable divergence concerns the definition of scientific research. In contrast with the UK's deliberately broad, and now more clearly articulated definition, the EDPB has set out a six-factor test requiring a methodical and systematic approach; adherence to ethical standards; verifiability and transparency; autonomy and independence; research objectives that contribute to society's general knowledge and wellbeing; and potential to contribute to or apply existing scientific knowledge in novel ways. While profit-making research can qualify, internal analytics for marketing or product promotion would not. The UK's simpler test is accordingly more permissive and is likely to capture a wider range of commercial research activities.

On consent, both regimes recognise "broad consent" to research, but the EDPB explicitly requires additional safeguards to compensate for the lack of purpose specification – including making detailed processing information available to data subjects as projects progress, time-limited validity of consent, and engaging independent oversight bodies that the UK does not impose. So the EU threshold is materially higher in this area.

On storage limitation, the EDPB requires that potential research purposes be reasonably foreseeable and sufficiently specific – retention for "generic scientific research purposes only" is not sufficient. The UK's framework, permitting indefinite retention with appropriate safeguards, is again more permissive.

The practical implication for organisations operating under both regimes is that a dual-track compliance approach may be necessary. Activities that comfortably qualify as scientific research under the UK's broader definition may need to be assessed more carefully against the EDPB's six-factor test for EU purposes. Consent mechanisms designed for the UK may need to be supplemented with additional safeguards to meet the EDPB's higher threshold. However, compared with the previous patchwork of national approaches across EU member states, the EDPB Guidelines offer a more predictable framework for cross-border research.

What's next?

On the evidence of the draft Guidance, the UK framework is becoming cautiously more permissive. The broad statutory definition of scientific research, the presumption of compatibility for re-purposing data, and the extended disproportionate effort exemption, collectively represent a meaningful relaxation in favour of data-driven research, in contrast with the EDPB's more demanding framework. The safeguards framework, however, is substantive; exemptions must be applied carefully and on a case-by-case basis, and documentation requirements remain considerable.

Once the consultation closes, and the Guidance is finalised, it will provide the most comprehensive regulatory framework to date for research-related data processing in the UK. Organisations should use the intervening period to review their current research processing activities against the Guidance, assess whether existing safeguards meet the standards set out, and ensure documentation - including records of lawful basis assessments, DPIA outcomes, and case-by-case exemption analyses - is robust and up to date. For organisations with cross-border operations, awareness of the UK and EU divergences will be essential to ensure compliant research practices across jurisdictions.

AUTHORS

Sarah O'Brien, Partner, Bobbie Bickerton, Managing Associate and Alison Llewellyn, Senior Knowledge Lawyer at Stephenson Harwood.
Emails:
sarah.obrien@stephensonharwood.com
bobbie.bickerton@stephensonharwood.com
alison.llewellyn@stephensonharwood.com

REFERENCES

1 ico.org.uk/for-organisations/research-archiving-and-statistics-provisions/
2 The consultation was due to close on 5 May 2026. Responses may be submitted via the ICO's Citizen Space online survey or by email to researchguidance@ico.org.uk.
3 ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/the-research-provisions/what-are-the-appropriate-safeguards/
4 www.edpb.europa.eu/our-work-tools/documents/public-consultations/2026/guidelines-12026-processing-personal-data_en

ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

When is AI 'high-risk'? The EU's draft guidelines

UK organisations operating globally must comply with the EU AI Act, which classifies AI into strict risk categories. **Emma Erskine-Fox** of TLT analyses the EU Commission's draft guidelines.

On 19 May 2026, the European Commission published draft guidelines[1] on how to classify Artificial Intelligence (AI) systems as "high-risk" under Article 6 of the EU AI Act, and opened a public consultation running until 23 June 2026. The high-risk AI obligations, particularly on providers, are extensive, and although the Digital Omnibus has pushed back the deadline for compliance

Continued on p.3

Data protection documentation – and where it fails

Data protection documentation is a comfort blanket where the means have become the ends, argues **Ralph O'Brien** of Serious Privacy.

There was a time when data protection was framed – at least in theory – as a means of safeguarding individuals' fundamental rights and freedoms. The UK GDPR still reflects that ambition, placing rights, fairness, and accountability at its core. Yet, in practice, compliance has increasingly become an evidence-based exercise, where the ability to *demonstrate* compliance often takes precedence over the substance of actually *achieving* the intent of the law.

Continued on p.6

Issue 146 **JULY 2026**

COMMENT

2 - UK follows Australia to ban social media for under 16s

NEWS

11 - ICO updates AI plans for 2026/27

ANALYSIS

1 - When is AI 'high-risk'? The EU's draft guidelines
8 - A more permissive UK framework for life sciences research data?
15 - Beyond the OSA / DSA: Age assurance as a data privacy duty
18 - Using blockchain requires data protection by design
21 - Should the EU's adequacy criteria for international data transfers be changed? If so, how?

MANAGEMENT

1 - DP documentation – and where it fails
12 - Behind the front door: When property data becomes personal
23 - Events Diary

NEWS IN BRIEF

5 - Social media for under 16s
5 - £600,000 OSA fine for porn company
14 - Digital Regulation Cooperation Forum seeks views on tools to manage risks with AI
14 - ICO advises government on PECR changes
17 - John Edwards resigns, Deputy Commissioner takes control for now
20 - DUAA: Complaints procedure should now be in place
23 - ICO advises on increasing AI cyber threats

See the publisher's blog at privacylaws.com/blog2026jul

UNITED KINGDOM
report

ISSUE NO 146 **JULY 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
Emma Erskine-Fox
TLT
Ralph O'Brien
Serious Privacy Ltd
Sarah O'Brien, Bobbie Bickerton and Alison Llewellyn
Stephenson Harwood
Patrick Arben, Jocelyn S Paulley, Loretta Pugh, Amber Strickland, Louise Macdonald and Isabel Roberts
Gowling WLG
Rebecca Cousin, Cindy Knott and Bryony Bacon
Slaughter and May
Nicola Fulford
Hogan Lovells
Sanjana Shikhar
The London School of Economics and Political Science

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

UK follows Australia to ban social media for under 16s

On 15 June, the government announced that by spring 2027, it will be unlawful for children under the age of 16 to have social media accounts (p.5). This move follows a wide public consultation, enforcement of the Online Safety Act by Ofcom (p.5) and ICO action in enforcing the Children's Code.

In March, the ICO wrote to TikTok, Snapchat, Facebook, Instagram, YouTube and X and called for them to urgently review and strengthen their age assurance measures to prevent underage children from accessing their services. Organisations now need to be alert to the ICO's increased appetite to enforce in this field. As our correspondents say, the more sophisticated age assurance technologies collect more data about the individual and therefore face their own data protection risks (p.15).

With the resignation of John Edwards, the ICO faces an uncertain time (p.17). When will we see the new ICO strategy, mandated by the Data (Use and Access) Act, and when will a new Information Commissioner be in place? DSIT also needs to issue the names of the seven non-Executive Directors for the ICO board. Not an ideal situation for anyone concerned.

In the meantime, DSIT is seeking a "data transfer fellow" for a secondment opportunity. "This role is designed for an ambitious individual to support the work of the team developing the legal mechanisms for data, with models for assessing the impact of current and future interventions in international flows," DSIT says. Will we soon see some new transfer tools perhaps? The placement will begin in the autumn.

The King's speech in May did not promise AI regulation but new regulatory sandbox powers. This will allow businesses to test new products and technologies in a controlled environment – to be legislated via the Regulating for Growth Bill. The UK's sectoral and light-touch AI approach means that organisations may look up to the EU for AI guidance. The EU AI Act's extra-territorial effect catches many UK organisations, and now there is clarification of "high risk" (p.1).

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.

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

"In a fast-moving and complex field with competing publications, *PL&B* stands out for its depth, independence, and authority. I have worked in several different industries operating in different geographical markets and would recommend both publications as essential reading for anyone working or advising on privacy, data protection and related matters."

Jane Hunt, Bauer Media Outdoor – Data Protection Officer

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.