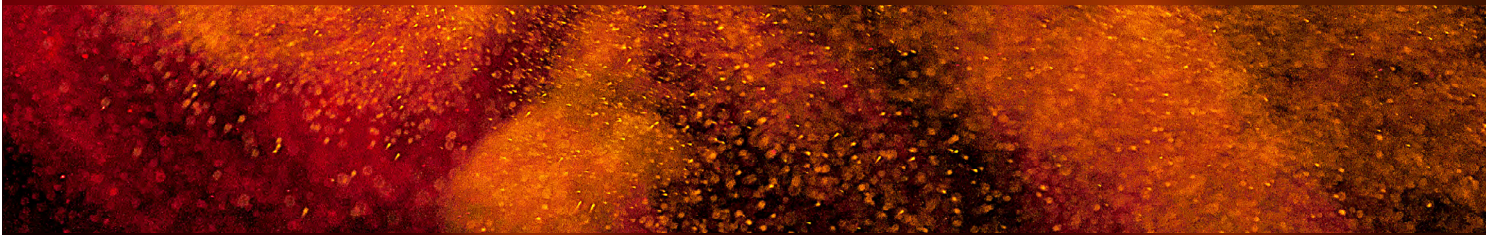


C L I F F O R D

C H A N C E



**UK DATA REFORM:
WHAT YOU NEED TO KNOW ABOUT THE DATA (USE AND ACCESS) ACT**

UK DATA REFORM: WHAT YOU NEED TO KNOW ABOUT THE DATA (USE AND ACCESS) ACT

After an eventful three-year legislative voyage, the UK's Data (Use and Access) Act 2025 (DUA Act) received Royal Assent on 19 June 2025. While most of the changes will be brought in through secondary legislation, a few limited provisions are already in force and others will come into force on 19 August 2025 (see our [timeline](#) below).

The DUA Act introduces wide-ranging and significant changes. In addition to amending UK data protection laws, the DUA Act establishes frameworks for 'smart data' schemes and a new regime for Digital Verification Services (DVS).

Overview

Smart Data: Building on the Smart Data Working Group's policy paper (published in Spring 2021), the DUA Act lays out a framework for the establishment of smart data schemes in the UK. While the detail of these schemes is to be set out in secondary legislation, they are potentially very broad and applicable beyond personal data.

Digital Verification Services: A framework to support digital identity verification in the UK, including rules for the provision of DVS and a public register of service providers.

Changes to the UK data protection regime include:

- **Automated decision-making:** relaxing the general prohibition on the use of personal data for significant automated decision-making (provided this is not based on special category data);
- **Facilitating data processing:** lowering the compliance burden and/or providing additional clarity for certain personal data processing (including for the prevention and detection of crime) – for example, see below on [recognised legitimate interests](#), [purpose compatibility](#) and [scientific research](#);
- **International data transfer:** reformulating the test for assessing a third country's adequacy in connection with international data transfer;
- **Complaints:** enabling data subjects to complain directly to controllers;
- **Clarifications:** codifying recitals and regulatory guidance (e.g., regarding [children's privacy](#) and [responses to data subject requests](#)); and
- **The Information Commissioner's Office (ICO):** The ICO is to be restructured, renamed and gains new enforcement powers. In performing its duties, it will need to consider (among other things) promoting competition and innovation.

Changes to PECR: The enforcement regime for the Privacy and Electronic Communications Regulations (PECR), which regulate cookies and electronic direct marketing, is aligned with that of the UK GDPR and the Data Protection Act 2018. Notably, this includes increasing potential PECR fines to UK GDPR levels. **Certain cookies** (e.g., for statistical purposes) are now expressly permitted without the requirement for consent.

Other provisions in the DUA Act range from digitising registers of births and deaths, to new crimes for creating intimate deepfake images, to requiring the Government to publish a report on the economic impact of the policy options set out in the Copyright and AI Consultation Paper.

How did we get here?

The predecessor to the DUA Act – the Data Protection and Digital Information Bill (DPDI Bill) – was first [introduced to the UK Parliament](#) in 2022 following a [public consultation](#) and government [response](#) on reforming the UK's data protection laws. Following a pause for input from business leaders and data experts, the DPDI Bill was reintroduced in March 2024 but did not complete during that parliamentary session. Instead, the Data (Use and Access) Bill (DUA Bill), which contained many similar provisions, was introduced in October 2024 (see our [comparative briefing](#) on the DUA Bill and the DPDI Bill). Several amendments were debated during the legislative process but few made it into the final text of the DUA Act. Notably, Baroness Kidron's proposals to mandate transparency in respect of copyright works used in pre-training, training and fine-tuning AI models, which delayed the passage of the DUA Bill for a couple of months, are not reflected.

What happens next?

Most of the DUA Act's changes are yet to be brought into force or otherwise apply only when secondary legislation is made. So far, only one commencement regulation has been made: [The Data \(Use and Access\) Act 2025 \(Commencement No. 1\) Regulations 2025](#). This brings a number of provisions into effect on 20 August 2025 (see our timeline below).

We understand that the Government's general plan is to commence: (i) the DVS provisions in September or October 2025; (ii) the substantive data protection provisions around December 2025; and (iii) provisions that require technology implementations, and the privacy complaints provisions in 2026 (or later).

In the interim, the ICO has [released high-level remarks](#) on the DUA Act as well as a [timetable](#) setting out when we should expect it to publish updated guidance in light of the various changes introduced in the DUA Act.

Known dates

19 JUNE 2025

Provisions that entered into effect include:

- Provisions stating that controllers need only conduct a "reasonable and proportionate search" on receipt of a subject access request.
- Provisions empowering the Secretary of State to make regulations. The Secretary of State will use these powers to bring into force the various aspects of the DUA Act over time.

19 AUGUST 2025

Provisions that enter into effect include those granting the ICO powers to require the provision of documents and to issue interview notices.

20 AUGUST 2025

Various provisions come into effect pursuant to [The Data \(Use and Access\) Act 2025 \(Commencement No. 1\) Regulations 2025](#). These include, for example:

- Provisions establishing the "Information Commission" (IC) – a body corporate to replace the ICO – as well as provisions amending the duties of the Commissioner when carrying out their functions and requiring the Commissioner to produce an annual report on regulatory action.
- The framework for smart data schemes in Part 1 of the DUA Act, to the extent not already in effect (although these provisions largely grant powers to the Secretary of State or the Treasury to make regulations, rather than directly implementing smart data schemes – powers which have not yet been exercised).
- Provisions stating that, where a court is required to determine whether a data subject is entitled to information by virtue of certain rights under the UK GDPR (e.g., the right of access and right to data portability) the court may require the controller to make available for inspection by the court "so much of the information as is available to the controller".
- Provisions updating PECR and Regulation (EU) 611/2013 to require providers of public telecommunication services to report personal data breaches to the IC without undue delay, and where feasible, no later than 72 hours of becoming aware of the breach.

- Provisions requiring the Secretary of State to publish a report assessing the economic impact of the policy options set out in the Copyright and AI Consultation Paper and a report on the effect of copyright on the development of AI systems within 9 months of commencement of the DUA Act, with a progress statement within 6 months.

SUMMER 2025

- The ICO is expected to release:
 - An “eIDAS – Revisions to ICO eIDAS Guide”.
 - “Profiling for Online Safety” guidance.

AUTUMN 2025

- On 15 September 2025 the Department for Science Innovation and Technology’s call for evidence on smart data opportunities in digital markets closes.
- The ICO is expected to release guidance on encryption.

WINTER 2025/2026

- The ICO is expected to release:
 - Detailed guidance on the right of access.
 - Complaints guidance for organisations.
 - Guidance on the DUA Act’s new legal basis of recognised legitimate interests.
 - Updated guidance on international transfers.
 - A “legitimate interest update”.
 - A Research, Archiving and Statistics Provisions update.
 - Updated guidance on the purpose limitation principle.
 - An update to direct marketing and privacy and electronic communications guidance.
 - Sectoral guidance on sharing information to safeguard children.
 - An interactive tool for “Substantial Public Interest Conditions”.
 - Guidance on the use of anonymisation and pseudonymisation for research purposes.
 - DUA Act updates to draft guidance on storage and access technologies (Part 2) – although this may end up coming out after Part 1 (see below).

SPRING 2026

- The ICO is expected to release:
 - DUA Act updates to draft guidance on storage and access technologies (Part 1).
 - An Automated Decision-Making (ADM) and Profiling Guidance update.

The details

01

Framework for smart data schemes

The DUA Act lays out a framework for the establishment of ‘smart data’ schemes in the UK, which are intended to promote competition between providers of goods, services and digital content by requiring data holders to take certain steps in connection with customer data and/or business data. These provisions only establish the framework for smart data schemes: the details of these requirements, their scope and enforcement regime, will be set out in secondary legislation which the Secretary of State is now empowered to make.

The smart data regimes will apply to “customer data” and/or “business data” – both of which are very broadly defined:

- “Customer data” is information relating to a customer of a trader (with a “trader” defined as a person who supplies or provides goods, services or digital content in the course of a business).
- “Business data” includes information about goods, services and digital content supplied or provided by the trader, and information relating to their supply (e.g., prices or other terms, how they are used, their performance or quality) and related feedback.

Data holders (i.e., traders or persons who process customer data or business data in the course of a business) may, for example, be required to:

- provide customer and/or business data either directly to the relevant customer, or to a person authorised by such customer to receive the data, at the request of the customer or the third party;
- produce, collect or retain customer and/or business data;
- make changes to customer data, including rectifying inaccurate data;
- use specified facilities or services (including, potentially, dashboard services, other electronic communication services or application programming interfaces), to facilitate data access and use; and
- create complaint-handling and dispute resolution procedures.

Such regulations may require a public authority that is a recipient of business data to take certain steps (e.g., to publish the business data.) They may also set out circumstances in which a data holder “may or must” refuse a data sharing request.

Unlike the EU’s Data Act, which focuses on data access and re-use in relation to a particular type of technology (i.e., access to and re-use of data concerning the performance, use and environment of connected products and related services), the legislation to be passed under the DUA Act is expected to be technology-neutral but tailored to specific sectors. It remains to be seen whether sectors prioritised for smart data schemes will align with the [Smart Data Roadmap](#) for 2024-2025, published by the UK’s Department of Business and Trade in April 2024, which identified ‘priority sectors’ including finance, banking, energy, telecoms and transport as well as ‘sectors of interest’ including retail.

Given that the UK banking sector has operated a smart data scheme since 2018, and the central role played by the Financial Conduct Authority (FCA) in open banking since then, the DUA Act reserves an important role for the FCA in the administration of smart data regimes in the financial services sector. The DUA Act provides for the Treasury to make regulations enabling or requiring the FCA to make specific rules governing how customer and business data is shared by financial services providers. The DUA Act empowers the Treasury to require the FCA to consult with the Payment Systems Regulator, the Bank of England and the Prudential Regulation Authority, with a view to ensuring a co-ordinated approach in the exercise of their respective functions with respect to the regulation of payment systems.

02

Digital Verification Services framework

To provide the legislative basis for the Government's ongoing work in building a digital identity ecosystem for the UK, the DUA Act introduces a new regime for DVS. The regime consists of five components:

- 1. Trust framework:** The Secretary of State will, in conjunction with consultations with the Information Commission (see section 4 below), prepare and publish a trust framework (rules and standards for the provision of DVS).
- 2. Supplementary codes:** Sets of rules to supplement the trust framework are to be published by the Secretary of State following consultation with the Information Commission and others as appropriate. Different DVS may be subject to different supplementary codes and supplementary codes may come into effect at different times for different purposes.
- 3. Register:** The Secretary of State will establish and maintain a **DVS register**, listing bodies that provide DVS services, and making it publicly available. To be listed on the register, DVS bodies would need to satisfy certain criteria, including holding a certificate issued by an accredited conformity assessment body.
- 4. Information gateway:** The information gateway will allow public authorities to disclose information to a registered DVS provider for the purpose of digital verification.
- 5. Trust mark:** The Secretary of State will have the power to designate a trust mark to be used only by those organisations on the DVS register.

Relevant to the DVS framework, the Office for Digital Identities and Attributes (OfDIA) was recently launched within the Department for Science, Innovation and Technology. The OfDIA will exercise the powers vested in the Secretary of State under the new DVS regime.

The DVS framework aims to facilitate commerce by speeding up the processes by which individuals open accounts with service providers and engage in transactions – such as moving house, undergoing pre-employment checks and buying or accessing age-restricted goods and services – thereby reducing the burden on consumers and businesses.

03

Changes to UK data protection laws

Set out below are some of the key changes made by the DUA Act to the UK GDPR and the Data Protection Act 2018.

New opportunities to use automated decision-making techniques

The DUA Act relaxes the existing general prohibition on the use of solely automated decision-making (ADM) for significant (e.g., legal) decisions affecting data subjects so that it applies only to significant ADM based entirely or partly on the processing of “special category” data (rather than restricting such decision-making based on personal data generally).

Significant ADM that is based on special category data will need to continue to rely on specific, limited legal bases for processing under UK GDPR (e.g., explicit consent). However, once these provisions come into force (on such day as the Secretary of State may appoint by regulation), the legal bases available for significant ADM that is not based on special category data will be wider (and will include ‘legitimate interest’).

Safeguards (such as transparency and contestability requirements) will apply to all significant ADM, not only those based on processing special category data.

The Secretary of State may, by regulation, specify certain decisions as having the required “significant effect” for the data subject (thereby triggering the safeguards for automated processing) and add to, or vary, the requirements in relation to the safeguards.

Provision for regulating novel types of special category data

The DUA Act inserts a new Article 11A into the UK GDPR which allows the Secretary of State to, by regulation, add (and, potentially, subsequently remove) additional categories of special category data.

This provision adds some flexibility into the law so that, as technology emerges and novel types of personal data come into existence, it can be clarified whether or not such personal data is special category data.

Skip the ‘balancing test’ when relying on ‘recognised legitimate interests’

The DUA Act introduces a new legal basis for personal data processing: ‘recognised legitimate interests’. Those set out in the DUA Act include processing necessary for; (i) responding to certain requests made by bodies acting in the public interest; (ii) national security, public security and defence purposes; (iii) the detection, investigation or prevention of crime; or (iv) the safeguarding of vulnerable individuals. Once these provisions enter into force (on such day as the Secretary of State may appoint by regulation) processing based on ‘recognised legitimate interests’ will satisfy the UK GDPR requirement to process personal data under a legal basis *without* the need to conduct a ‘balancing test’. The Secretary of State may make regulations adding to, or varying, these ‘recognised legitimate interests’. ICO guidance on the new legal basis of ‘recognised legitimate interests’ is expected to be published in Winter 2025/2026.

The DUA Act also clarifies that processing: (a) necessary for the purposes of direct marketing; (b) involving intragroup transmission of personal data where this is necessary for internal administrative purposes; or (c) necessary for ensuring the security of networks and IT systems, can be based on the (pre-existing) legitimate interests legal basis, subject to the usual balancing test. This essentially imports clarificatory provisions already included in the recitals to the UK GDPR into its main text.

Additional clarity on purpose limitation and further processing

The DUA Act clarifies the circumstances under which an organisation is allowed to reuse personal data for purposes that are different to those for which the data was originally processed.

The DUA Act adds provisions and an annex to the UK GDPR which together specify certain circumstances in which further processing of personal data for a new purpose satisfies 'purpose compatibility' requirements. Depending on the legal basis relied on for the original processing, these can include, for example, further processing for research, archiving or statistical purposes, public security, detecting, investigating or preventing crime, safeguarding vulnerable individuals, the assessment or collection of tax, and complying with a legal obligation or court / tribunal order. The Secretary of State may add to or modify this list of compatible processing.

The DUA Act also sets out factors that controllers are to consider when determining "purpose compatibility" for data reuse in other circumstances. These include, for example, any link between the original purpose and the new purpose, the possible consequences for data subjects of the proposed processing, and the existence of appropriate safeguards (for example, encryption or pseudonymisation). This provision primarily provides additional clarity as to how the purpose limitation principle is to be applied in practice.

Additional clarity on processing for research and statistical purposes

The DUA Act defines "research and statistical purposes" to include "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". Once brought into effect by secondary legislation, this aligns the substantive provisions of the UK GDPR with existing recitals and regulatory guidance to encourage a broad interpretation of the concept of scientific research, such that the UK GDPR's purpose limitation principle, and its restrictions on the processing of special category data, are less likely to restrict processing for such purposes provided certain safeguards are met. The DUA Act also clarifies that data subjects can give "broad consent" for processing of their data for an area of scientific research in certain circumstances.

The "data protection test" for international transfers

The DUA Act reformulates the existing regime restricting the international transfer of personal data in the UK GDPR, for the most part by restating the existing provisions in a clearer manner. Most importantly, the DUA Act introduces a "data protection test" to be applied by the Secretary of State when deciding whether to approve by regulations international data transfers to a third country, including by way of recognising a third country's data protection regime as adequate. Once these provisions enter into force (on such day as the Secretary of State may appoint by regulation), the Secretary of State will be required to assess whether the standard of protection in a third country or otherwise in place in respect of a transfer is "not materially lower" than the standard in the UK. The data protection test is also to be applied by controllers and processors before they may transfer personal data to a third country in reliance on "appropriate safeguards" (such as standard contractual clauses).

This may amount to a slightly lower standard than the “essential equivalence” test referred to in the EDPB’s guidance – and in judgments of European Union courts – on risk assessments for international transfers of personal data, but it remains to be seen whether this will prove a meaningful distinction. The UK will be mindful that differing standards for the export of personal data from EEA jurisdictions versus that from the UK may complicate data governance and be subject to scrutiny.

The DUA Act also provides that, when approving transfers by regulations, the Secretary of State may also consider other ‘matters’ it deems relevant, including the “desirability of facilitating transfers of personal data” to or from the UK, and empowers the Secretary of State to recognise new transfer mechanisms for international data transfers.

Additional clarity on obligations when responding to subject access requests

The DUA Act codifies rules that currently exist only in regulatory guidance as to: (a) when a controller can ‘stop the clock’ in calculating the applicable time frame for responding to the exercise of a data subject’s right; and (b) the obligation on the controller to perform (only) a “reasonable and proportionate search” for personal data in response to a subject access request. For organisations already following ICO guidance on subject access requests, this will likely not be a material change.

Permitting processing performed in reliance on international treaties

The DUA Act broadens the circumstances in which processing may be based on a legal obligation to include not only domestic law but also relevant international law. For the time being, “relevant international law” refers only to the Agreement between the UK-USA Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime, but the Secretary of State is empowered to add other treaties ratified by the UK in future.

Children’s privacy

The DUA Act obliges controllers providing information society services likely to be accessed by children to consider ‘children’s higher protection matters’ when determining what measures are appropriate to ensure data protection by design and default. In line with the ICO’s Children’s Code, these measures include how children can best be protected when using the services and the fact that children merit specific protection, because they may be less aware of certain risks and consequences, and less aware of their rights, and have different needs at different ages.

04

Enforcement and regulatory engagement

The “Information Commission”: role and powers

The ICO will be replaced with an “Information Commission”, which will be a body more closely resembling other statutory regulators such as Ofcom and the Competition and Markets Authority. In carrying out its duties, the Information Commission must have regard to:

- promoting innovation;
- promoting competition;
- the importance of preventing, investigating, detecting and prosecuting crime;
- the need to safeguard public security and national security; and
- the fact that children may be less aware of the risks and consequences associated with the processing of personal data and of their rights in relation to such processing.

These considerations appear to be intended to promote a pragmatic, ‘growth-friendly’ approach to regulation and oversight. While these provisions are not yet in force, the ICO’s strategic plans suggest that, to a large extent, it is already having regard to these matters.

The DUA Act adds to the Information Commission’s regulatory toolkit by giving it powers which include: (a) requiring that a controller or processor not only provide it with information, but specific documents (this provision comes into force on 19 August 2025) and/or require the preparation of a report, at the expense of the controller or processor being investigated; and (b) issuing an interview notice, compelling a witness to attend interview, where giving a false statement in response to an interview question would be an offence (this provision also comes into force on 19 August 2025).

Privacy complaints can go straight to controllers

The DUA Act creates a right for data subjects to complain directly to controllers in relation to infringements of data protection law. Once brought into force by secondary legislation, this will exist alongside the existing ability to lodge complaints with the ICO.

The DUA Act will require controllers to facilitate the making of such complaints, e.g., by providing a complaint form “which can be completed electronically and by other means”; and to acknowledge complaints within 30 days, to take appropriate steps to resolve the complaint without undue delay, and inform the data subject of both progress and the outcome. The DUA Act also allows for regulations to be made mandating controllers to report to the new Information Commissioner the number of complaints received within specific periods.

PECR enforcement to be aligned with UK GDPR enforcement

The DUA Act updates the UK’s ePrivacy enforcement regime, under the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR), bringing it in line with the UK GDPR and Data Protection Act 2018. Notably, this means the potential PECR fines will increase to UK GDPR levels once these provisions are brought into force by secondary legislation.

05

Cookies, trackers and security patches

Provision for low-risk cookies and trackers

The DUA Act introduces new provisions that clarify and expand the circumstances in which consent for cookies under PECR will not be required. At present, PECR requires consent for storage of, or access to, information within terminal equipment (e.g., phones, browsers) via cookies, trackers and similar technologies. Currently, PECR provides an exception for cookies that: (a) are “strictly necessary” for the user or subscriber to receive the service they have requested from the service provider; or (b) have the sole purpose of transmission of a communication across a network.

Under the DUA Act, the circumstances in which it will not be necessary to obtain such consent to store or access information include:

- statistical / analytics cookies – that gather information about how a website or digital service is used with a view to making improvements to the website or service (subject to information provision and the ability to object);
- personalisation / appearance cookies – that automatically authenticate a repeat user of a digital service or repeat visitor to a website and/or maintain a record of settings or preferences that the user has set to save the user the effort of setting those settings or preferences each time they return (subject to information provision and the ability to object);
- strictly necessary cookies – the DUA Act clarifies that cookies that are strictly necessary to provide a service requested by the user include, for example, the following use cases: (i) preventing or detecting fraud in connection with providing the service; (ii) preventing or detecting technical faults when providing the service; or (iii) automatically authenticating the identity of the user; and
- other cookies – cookies to find the geolocation of the user of a device to provide emergency assistance to the individual.

While taking advantage of these exemptions in the UK could provide a more streamlined user experience and reduce consent requests, as well as making it easier to roll out security-related software updates, implementing a separate system for the UK to that used for the rest of Europe could lead to increased complexity and operational costs. These factors would need to be weighed in any operational decision to take advantage of the exemptions.

06

Other provisions

The DUA Act includes a number of other provisions which include, for example:

Copyright and AI – emerging issues to be addressed outside the DUA Act

There was prolonged debate after Baroness Kidron put forward proposals to include provisions mandating transparency in respect of the copyright works used in pre-training, training and fine-tuning AI models, despite a parallel consultation process on copyright and AI taking place. These were not ultimately reflected in the final text.

However, the DUA Act does require the Government to publish a report addressing the economic impact of the policy options set out in the Copyright and AI Consultation Paper and consider the effect of copyright on the development of AI systems. The report must be ready by 19 March 2026, with a progress report to Parliament in December 2025.

Facilitating research into online safety

The DUA Act amends the Online Safety Act 2023, empowering the Secretary of State to make regulations requiring providers of internet services to share information for independent research into online safety matters. Those regulations are to set out the criteria, application and handling requirements for the provision of such information.

Investigating children’s deaths that may be related to their online activities

The DUA Act amends the Online Safety Act 2023 to provide for a coroner investigating the death of a child to notify Ofcom, and for Ofcom to require internet service providers of certain regulated services to retain information relating to the use of that service by the deceased child.

New information standards in health and social care

Currently, health and social care providers can face challenges in accessing or sharing patient care-related information due to, for example, inconsistencies in data and system interoperability challenges. Reforms included in the Health and Care Act 2022 made information standards mandatory and extended their application to private health and care providers. The DUA Act extends the scope of information standards further, so they apply also to IT suppliers of systems and services used in the health and adult social care system.

Mapping what’s underground

The DUA Act provides a legislative basis for the existing National Underground Asset Register (NUAR) of infrastructure below street level, such as electricity and utility cables and water pipes. The information included in NUAR is prescribed in regulation and the >600 owners of underground assets will be required to upload such information into the NUAR.

Smart meter communication services

The DUA Act amends energy, gas and electricity laws to empower the Gas and Electricity Markets Authority (Ofgem) to administer smart meter communication licences. These licences support the telecommunications networks to which smart meter devices connect.

Data for improving public service delivery

The DUA Act amends the Digital Economy Act 2017 such that public bodies may disclose information for purposes of improving public service delivery to undertakings (in addition to existing provisions allowing this in relation to individuals and households).

Digitising births and deaths registers

The DUA Act supports the complete digitisation of registers of births and deaths.

New crimes for creating or soliciting intimate images

The DUA Act amends the Sexual Offences Act 2003 to create new offences in relation to the creation of deepfake intimate images without consent from the person depicted.

Takeaways for businesses and other organisations

Organisations should monitor secondary legislation passed under the DUA Act (and any related consultations or engagement) to understand when the changes that are not already in force will be brought in and monitor upcoming ICO guidance (see our [timeline](#)). In addition, organisations should consider the preparatory steps below.

1. Review UK data governance compliance processes

Organisations should review their data protection processes, notices and internal guidance in light of:

- upcoming obligations that require updates to policies and workflows – such as the requirement that controllers put in place an electronic complaint-handling mechanism; and
- additional clarity organisations may have in areas where recitals and regulatory guidance have been codified into the law – such as in relation to responding to data subject requests and considerations for children’s privacy.

2. Prepare for divergence from the EU GDPR and ePrivacy Directive

The DUA Act includes some steps away from EU data protection norms, such as the broader range of legal bases available for significant ADM in many circumstances, the ability to rely on certain recognised legitimate interests and some nuances regarding assessments that accompany international data transfers. It also allows for use of a broader range of cookies without consent and changes the maximum potential fines for PECR infringements.

In most cases, compliance with requirements under EU privacy-related laws will also mean compliance with the UK regime but organisations should:

- identify any instances where a change is mandatory (e.g., see above in relation to privacy complaints); and
- in other cases, where maintaining existing processes would remain compliant under UK laws, organisations should consider whether any data processing activities or cookie use would benefit sufficiently from the changes introduced by the DUA Act that it is worth implementing operational divergence. Organisations that are also subject to EU laws will need to consider possible complexities introduced by dual compliance processes and whether they need to carry out any data segregation to operate different processes for data that is subject only to UK law.

Organisations should also review any risk-based decisions they may have made based on the previous PECR enforcement regime.

3. Monitor sector-specific data sharing provisions

Businesses should monitor especially closely the progress of initiatives to implement smart data schemes in the UK, in particular any secondary legislation passed relating to the sectors in which they operate and related consultations or engagement processes. These could introduce significant operational requirements in respect of customer data and/or business data, as well as potential opportunities for businesses receiving such data. Engagement with regulators and industry bodies may help shape these schemes.

CONTACTS



Jonathan Kewley
Partner and Co-Chair of
the Global Tech Group
London
T: +44 207006 3629
E: jonathan.kewley@
cliffordchance.com



Herbert Swaniker
Partner
London
T: +44 207006 6215
E: herbert.swaniker@
cliffordchance.com



James Wong
Lawyer (Country
Qualified: Australia)
London
T: +44 207006 3750
E: James.Wong@
cliffordchance.com



Rita Flakoll
Knowledge Director
London
T: +44 207006 1826
E: Rita.Flakoll@
cliffordchance.com

C L I F F O R D

C H A N C E

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

© Clifford Chance 2025

Clifford Chance LLP is a limited liability partnership registered in England and Wales under number OC323571

Registered office: 10 Upper Bank Street, London, E14 5JJ

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications

If you do not wish to receive further information from Clifford Chance about events or legal developments which we believe may be of interest to you, please either send an email to nomorecontact@cliffordchance.com or by post at Clifford Chance LLP, 10 Upper Bank Street, Canary Wharf, London E14 5JJ

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Houston • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague • Riyadh* • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

*AS&H Clifford Chance, a joint venture entered into by Clifford Chance LLP.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.