STEPHENSON HARWOOD

July 2025

THE DATA (USE AND ACCESS) ACT 2025

OVERVIEW OF THE LAW

On 19 June 2025, the Data (Use and Access) Act 2025 (the "**DUAA**") received Royal Assent and became law in the UK.

The DUAA will facilitate the safe and effective use of data, encourage innovation and simplify data protection. It amends and supplements, but will not completely replace, the UK General Data Protection Regulation ("**UK GDPR**"), Data Protection Act 2018 ("**DPA 2018**") and the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("**PECR**").

A key aim of the DUAA is to strengthen both data safeguards and transparency in the UK. It supports the UK's efforts to maintain its data adequacy status with the European Union ("**EU**") despite minor divergences from EU law.

WHEN DOES IT COME INTO EFFECT?

Certain provisions in the DUAA came into force immediately on 19 June 2025, including the requirement for "reasonable and proportionate" searches to be made when responding to data subject access requests ("**DSARs**"). A number of primarily administrative provisions come into force on 20 August 2025, with the remaining substantive data protection changes expected to be phased in on or around December 2025 via secondary legislation, with minority provisions thereafter.

WHAT WILL CHANGE?

A new Information Commission ("**IC**") will replace the Information Commissioner's Office ("**ICO**") as the UK's supervisory authority, featuring a formal board and CEO rather than being led by a single commissioner. John Edwards (the current Information Commissioner) will be Chair, with Paul Arnold appointed the first CEO of the IC.

It is worth noting that certain proposed amendments under the previous Data Protection and Digital Information Bill were not carried over to the DUAA. There is no change to the definition of "personal data" in the DUAA; Data Protection Officers, ROPAs and DPIA requirements will remain the same as under the existing law; and the ability for controllers to refuse to respond to a "*vexatious or excessive*" DSAR has been dropped.

WHAT DO I NEED TO KNOW?

Ten key reforms of the DUAA impacting the data protection and ePrivacy landscape, and an analysis of the implications of these changes, are summarised in the table below.

The DUAA also addresses the creation and implementation of legal frameworks for smart data schemes and the introduction of trusted digital verification services. Whilst the DUAA diverges from current law in certain areas in its aim to introduce greater flexibility, the changes actually introduced are relatively limited.

Where organisations already comply with the current UK data protection and ePrivacy regimes, it is unlikely that organisations will need to make significant adjustments. That said, the new mandatory complaints procedure is one of the few provisions in the DUAA that will require most organisations to take proactive steps to comply, and with the increased fines for infringements of ePrivacy rules, organisations would be well advised to review and ensure their existing UK processes are compliant.

Read our article series here covering key aspects of the DUAA

REFORM	SUMMARY	IMPLICATIONS FOR BUSINESSES
New mandatory complaints procedure	New statutory right for individuals to raise a complaint to a controller regarding their general UK GDPR compliance. Controllers must have clear processes to facilitate complaints, acknowledge receipt within a 30-day timeframe and respond "*without undue delay*".	Creates greater accountability and may increase operational burdens for organisations receiving high volumes of data-related queries. Business should consider implementing online complaints forms and additional staff training.
Strengthened and extended IC enforcement powers	The IC's assessment notice powers will be extended to enable the IC to interview individuals and require organisations to provide documents and prepare reports to assist in an investigation.	Additional operational burden underscores the importance of recordkeeping obligations and upholding the accountability principle.
Updates to DSAR obligations	Controllers can "stop the clock" when responding to a DSAR. A requirement that searches be "*reasonable and proportionate*" applies retrospectively from 1 January 2024.	Codifies rules contained in existing ICO guidance. A more pragmatic approach to responding to DSARs reduces the burden on organisations to conduct unreasonably broad searches.
New assessment for international transfers of personal data	Data protection standards in the destination jurisdiction for personal data transfers must not be "*materially lower*" than those in the UK.	Less stringent than the EU's requirement for "*essential equivalence*".
List of recognised legitimate interests	Balancing test no longer required for list of "recognised legitimate interests" (e.g. processing for national security, emergency response and safeguarding vulnerable individuals).	Controllers are exempt from conducting a full legitimate interests' assessment when processing personal data for specified purposes, albeit these are narrow in scope.
Clarity on purpose limitation	The purpose for which the controller making the assessment collected the data is key for assessing compatibility of any “further processing” with original purpose.	Provides clarity on how to ascertain compatibility with an original purpose.
Relaxation on solely automated decision making ("ADM")	Restrictions removed around significant decisions made solely by ADM, unless special category data is involved (in which case the current restrictions remain).	It may be permissible to carry out ADM in reliance on legitimate interests.
Increased PECR fines and changes to Cookies rules.	Fines for PECR infringements will be brought in line with the maximum fines that can be levied under the UK GDPR (£17.5m or 4% of annual turnover). Exceptions to consent requirements have been introduced for certain low-risk cookies (e.g. for statistical purposes and website functionality) but opt-out still required.	Businesses must strengthen compliance with electronic marketing and cookie regulations.
Broader definition of scientific research	"*Scientific research*" includes non-commercial and commercial scientific research. Broad consent for scientific research now permitted.	Data can be collected for general research purposes without specifying all future uses (which may not yet be known). Reduces barriers for businesses and research organisations using personal data.
"*Children's higher protection matters*" threshold	Greater obligations for providers of information society services likely to be accessed by children.	Increased compliance requirements, particularly around safety and data minimisation.

OUR TEAM

KATIE HEWSON

Partner

+ 44 20 7809 2374
katie.hewson
@stephensonharwood.com

JOANNE ELIELI

Partner

+ 44 20 7809 2594
joanne.elieli
@stephensonharwood.com

SARAH O'BRIEN

Managing associate

+ 44 20 7809 2481
sarah.o'brien
@stephensonharwood.com

BOBBIE BICKERTON

Managing associate

+ 44 20 7809 2140
bobbie.bickerton
@stephensonharwood.com

ALISON LLEWELLYN

Senior knowledge lawyer

+ 44 20 7809 2278
alison.llewellyn
@stephensonharwood.com

MATTHEW ANGELL

Associate

+ 44 20 7809 2669
matthew.angell
@stephensonharwood.com

TATIANA CORDILHA GHELFENSTEIN

Associate

+ 44 20 7809 2887
tatiana.ghelfenstein
@stephensonharwood.com

JONATHAN HOWIE

Associate

+ 44 20 7809 2337
jonathan.howie
@stephensonharwood.com

MONICA MYLORDOU

Associate

+ 44 20 7809 2242
monica.mylordou
@stephensonharwood.com

JOSEPH SAMUELSON

Associate

+ 44 20 7809 2117
joseph.samuelson
@stephensonharwood.com

THE LEGAL 500 UK, 2025

"The team's practical, actionable advice makes them unique - they combine deep technical knowledge with business savvy in a way that provides unmatched value to their clients."