OLIVIA WHITCROFT

"When I awoke, my post had over 100 reactions. Had I finally reached influencer status?"

A new data act clarifies many aspects of the law, but questions remain in a number of areas, as *PC Pro*'s newest influencer explains

I've never had as much engagement with my social media posts as I did when the Data Use and Access Act 2025 (DUA Act) received Royal Assent on 19 June. After waiting since Brexit and the government's 2021 consultation paper (Data: A New Direction) to find out which changes were coming, this was top news. I was delivering data protection training during the day so shared the excitement with delegates, but it wasn't until that evening that I posted on LinkedIn about the new law.

I don't use LinkedIn a lot, and I'm usually happy if I get a handful of likes. Last time I posted about the DUA Bill (as it then was), it had eight reactions and six comments. But when I awoke the next morning, my post had over 100 reactions and several comments. Had I finally reached influencer status? At last, the world was as enthused as me about data protection!

In my eagerness to share the news I hadn't phrased my opening line as well as I could, and someone had said it wasn't actually a new data protection law; it was a modification to existing law. And that's an important point. The DUA Act doesn't create an entirely new data protection regime. It amends the UK GDPR and the Data Protection Act 2018 (DPA), so we need to read it in that context. Down the line we won't be referring to sections of the DUA Act, but the new or amended sections of the UK GDPR and the DPA.

As I had hinted at in my post, it also isn't just about personal data. The Act makes reforms in relation to privacy and electronic communications (including direct marketing and cookies), smart data and digital verification services. It also tiptoes into copyright and AI, which received last-minute attention as the near-final Bill ping-ponged between the House of Commons and the House of Lords.

Olivia is principal of the law firm OBEP, which specialises in technology contracts, IP and data protection
@ObepOlivia

"At last, the world was as enthused as me about data protection!"

BELOW Who'd have thought that a post on data protection would go viral?

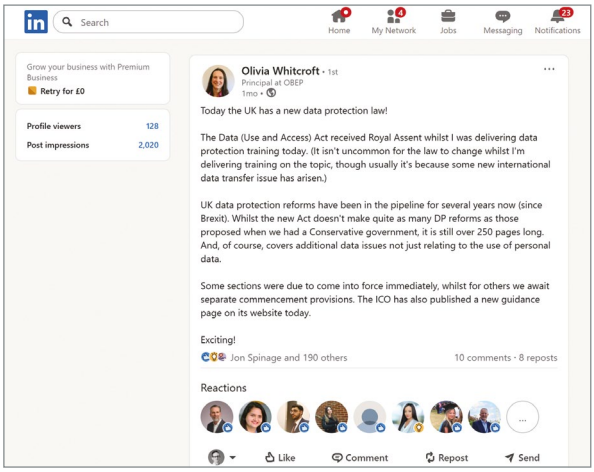
Some provisions came into effect immediately or in August, but, as I write, we still await commencement of the remaining provisions, expected over the next few months.

I talked about subject access requests in issue 369 of *PC Pro*, so have pulled out some other hot topics to tell you about here: international data transfers, automated decision-making and training of AI.

International data transfers

Schedules 7 to 9 of the DUA Act contain a lot of stuff on one of my favourite subjects: international data transfers. The government previously said the purpose of the changes was to allow a risk-based and flexible approach to transfers. But the provisions seem to focus on structural and linguistic modifications, rather than changing the key transfer mechanisms. One might wonder why they bothered to add 20 pages to the Act.

On more careful consideration, some potentially significant points emerge. There's a new "data protection test", which both the government and organisations must consider before making decisions on whether to allow transfers to non-UK countries. For organisations, this appears to embed transfer risk assessments (TRAs, arising from the Schrems II case) into legislation.



Under current law, the aim of the rules is to ensure that, when an international transfer is made, the level of protection for individuals is "not undermined" (Article 44 UK GDPR), and a non-UK country may be deemed adequate if the level of protection is "essentially equivalent" to that within the UK (or EU, as originally drafted – Recital 104 GDPR). The ICO's guidance on TRAs refers to people being in a "sufficiently similar" position in relation to the risks. The new data protection test requires the standard of protection to be "not materially lower" than in the UK.

What does this change mean? Is "not materially lower" different to "essentially equivalent" and "sufficiently similar", or is it just a new synonym stripped of the satisfying alliteration?

Also of note is that the data exporter must act "reasonably and proportionately" in determining whether the test is met. This may take into account the circumstances or likely circumstances of the transfer, including the nature and volume of personal data transferred. For those using the ICO's template for their TRAs, these factors are already built into the assessment.

So the practical impacts of these changes are not immediately clear. The UK's status as a country with adequate data protection laws is set to be reviewed by the EU in December, and I expect these data transfer changes will be scrutinised in deciding whether transfers into the UK from the EU continue to be permitted. I'll be interested in the EU's views on whether "not materially lower" is essentially equivalent to "essentially equivalent".

Early signs are positive. On 22 July, the EU Commission published a draft renewal of its adequacy decision for data transfers to the UK, indicating that UK data protection law, as amended by the DUA Act (including changes relating to data transfers, automated decision-making and research) continues to ensure a level of protection essentially equivalent to that in the EU.

Automated decision-making

The DUA Act significantly relaxes the rules on automated decision-making. Currently, under Article 22 UK GDPR, the rules are phrased as a prohibition. In short, subject to some exceptions, it isn't permitted for a software algorithm by itself to make a significant decision about an individual. Such decisions may relate to credit applications,

access to medical treatment or setting of insurance premiums, for instance.

I've also had many conversations about automated decisions in recruitment and employment matters. AI or other algorithms may be used to sift through large quantities of applications for a role, or analyse data for monitoring staff performance. Safeguards are often built in (such as allowing requests for human review), but it can be a hurdle identifying an exception to the prohibition. As I touched on in my article on lawful basis in issue 361, to be permitted, the automated decision must be necessary for entering into or performance of a contract with the individual, required or authorised by law, or based on the individual's explicit consent.

It's hard to argue that using AI to screen a CV is necessary for an employment contract, before the application is discarded without a human ever looking at it. At that stage, the contract is more a glint in the milkman's eye than something you're about to enter into. And, for an existing employee, can you demonstrate that the automated decision is necessary for the employment contract? There are some contexts in which automated decisions may be a good way to achieve something required by law, such as detecting fraud, but these are likely to be rarer.

That means we're left with explicit consent. But giving applicants or employees a genuine choice isn't as easy as it sounds. People may say yes just to stay on-side with you, or you may not really have a good alternative for someone who says no.

Under the new rules, the main prohibition will be for solely automated decisions based on special category data (such as information about health or ethnic origin), or that rely on a new lawful basis of "recognised legitimate interest" (also discussed in issue 361). For those based on special category data, there will be similar exceptions, with an additional public interest condition if explicit consent is not given. Safeguards must still be in place for all significant automated decisions, including explaining what you are doing and allowing individuals to contest the decision.

So we can get back on track with the law by considering other bases for automated decisions; in particular, "necessary for legitimate interests" (note this is different to recognised legitimate interest). We still have some points to check, though: is it a proportionate approach in context, such as a practical way to review thousands of CVs? Are the algorithms fair, and have risks of bias been mitigated in training of AI? Are individuals' rights protected? For example, have you told them it is happening, and can they challenge the decision? If yes to all of these, then my head can finally stop spinning in trying to find a lawful way for organisations to do increasingly commonplace activities.

AI, copyright and research

The AI and copyright issue bounced back and forth between the House of Commons and the House of Lords for the final few weeks of the DUA Bill. With references to *Groundhog Day* and *Macbeth*, the Hansard reports are quite fun to read. The Lords thought it a good opportunity to address this data-related issue within the data-related Bill. However, the Commons didn't think the Bill was the right place to tackle this matter and rejected the Lords' provisions several times. The Act ended up with some woolly obligations for an economic impact assessment on the options for changes to copyright law from the government's 2024 AI and copyright consultation (*see issue 369, p116*) and a report on the development of AI systems, such as technical measures to control use of copyright works.

The Lords had wanted to include transparency obligations in the use of works to train models, so that copyright law can be enforced where needed. They also sought to address a jurisdictional point, so that AI models trained or developed overseas but marketed in the UK or with significant UK users should comply with UK copyright law. These debates were happening alongside the *Getty Images v Stability AI* High Court case (*see issue 372, p116*). A key issue was – you got it – whether training of Stability AI's Stable Diffusion model took place inside or outside the UK and the extent to which UK copyright law applied. The key copyright claims were subsequently dropped due to a lack of evidence on this. Gah!

ABOVE **It remains unclear whether the training of AI counts as scientific research**

"The changes to automated decision-making rules have saved my head some spinning"

BELOW **The House of Lords tried to address the AI/copyright issue in the DUA Bill**

A related but less well-publicised debate on the DUA Bill concerned changes to the research provisions of data protection law. The re-use of personal data for scientific research is considered compatible with the purposes of collection, which means no additional consent is needed from individuals. The DUA Act clarifies that both commercial and non-commercial activities can be scientific research. The House of Lords was concerned that personal data may be scraped to train AI under the heading of "scientific research", so proposed that the research should have a public benefit, too. This was also ultimately rejected, and the final wording leaves us with the question of whether training of AI is research that could "reasonably be described as scientific".

Where does this get us?

The changes to automated decision-making rules have saved my head some spinning, but we aren't yet clearer on the practicalities of applying UK copyright law to the training of AI. And it seems my head can keep spinning for a bit on the meaning of "not materially lower" for international data transfers, and in what circumstances describing something as scientific research may be deemed "reasonable".

On a brighter note, as I write this, my LinkedIn post on the DUA Act has 191 reactions. I'm sure by the time this article is published it will have reached even dizzier heights, firmly establishing my pico-influencer status.

olivia.whitcroft@obep.uk