



# PRIVACY LAWS & BUSINESS

DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

## UK and EU – Cookie rules to become the ‘law of everything’?

**Greg Palmer** and **Ceyhun Necati Pehlivan** of Linklaters analyse the proposed changes to cookie provisions in the UK’s new Data (Use and Access) Bill, and the approach taken recently by the EDPB.

**H**elen Dixon, the former Irish Data Protection Commissioner famously described the GDPR as the “law of everything”. The broad scope of the concepts of “processing” and “personal data” means almost everything

any business does is subject to the GDPR.

Recent developments risk a similarly expansive application of the cookie rules. The UK’s Data (Use

*Continued on p.3*

## The ICO’s consultation on generative AI: Key take-aways

The ICO expects the industry to significantly improve how it informs individuals about data processing. By **Josephine Jay** and **Annabel Loose** of Goodwin.

**A**s the predominance of generative artificial intelligence (AI) continues to gather pace, legislators and advisory bodies face the challenge of fitting this technology into existing and emerging legal frameworks, without stifling

innovation. Amongst other things, the large-scale data processing driving generative AI raises complex questions regarding compliance with data protection laws, including the

*Continued on p.6*

### **Data Opportunities in Ireland**

Thursday 6 February  
McCann FitzGerald, Dublin

Speakers include Dr Des Hogan, Data Protection Commissioner, Ireland

Free for *PL&B* subscribers registering by 17 January.

[www.privacylaws.com/ireland2025/](http://www.privacylaws.com/ireland2025/)

Issue 137

JANUARY 2025

#### COMMENT

- 2 - Data (Use and Access) Bill may make life easier for business

#### NEWS

- 9 - New Data Bill will support wider data sharing
- 19 - Dame Wendy Hall: UK should not follow EU’s approach on AI
- 26 - Teens ask social media companies to protect their mental health

#### ANALYSIS

- 1 - UK and EU – Cookie rules to become the ‘law of everything’?
- 1 - ICO’s views on generative AI
- 12 - Data Bill: Automated decision-making in the spotlight
- 16 - The new UK approach: Making international transfers easier?
- 17 - A focus on the digital identity provisions in the DUA Bill

#### MANAGEMENT

- 11 - Events Diary
- 21 - Privacy by Design through certification and standards
- 23 - Risk, revenue, and relationships: A case study

#### NEWS IN BRIEF

- 5 - ICO comments on Data Bill
- 8 - Ofcom issues enforcement guidance on Online Safety Act
- 11 - DRCF monitors Quantum Technologies
- 18 - Court of Appeal rejects appeal against ICO’s Monetary Penalty Notice
- 20 - ICO consults on its approach to fines in the public sector

**PL&B Services:** Conferences • Roundtables • Content Writing  
Recruitment • Consulting • Training • Compliance Audits • Research • Reports

UNITED KINGDOM  
**report**

ISSUE NO 137

JANUARY 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**

**Greg Palmer and Ceyhun Necati Pehlivan**  
Linklaters

**Josephine Jay and Annabel Loose**  
Goodwin

**Fiona Maclean, Gail Crawford, Amy Smyth  
and Lorenzo Meusburger**  
Latham & Watkins

**Rachael Annear, Joseph Mason,  
Adam Gillert and Rhea Dennis**  
Freshfields

**Nicola Fulford**  
Hogan Lovells

**Ralph O'Brien**  
REINBO Consulting

**Lauren Reid**  
The Privacy Pro

**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

**Copyright:** No part of this publication in whole or in part may be reproduced or transmitted in any form without the prior written permission of the publisher.

© 2025 Privacy Laws & Business



## DUAB may make life easier for business

The new Data (Use and Access) Bill continues its passage through Parliament with the Report stage in the House of Lords on 21 and 28 January. In this issue our contributors look in more detail into four areas where there are some novelties; cookies (p.1), automated decision-making (p.12), digital identities (p.17) and international data transfers (p.16).

Some aspects of the Bill will be welcomed by DPOs such as the legitimate interest grounds for direct marketing, or narrowing SAR searches to what is “reasonable and proportionate”. It is also reassuring that there will be no changes to the DPO role, rejecting the proposals in the previous Bill.

But there are also open questions about the interpretation of some of the Bill’s wording, as was evident at the Bill Briefing event organised by *PL&B* with Linklaters (p.9). It may be that much of this work is left to the ICO in terms of issuing guidance. One area which generated a lively discussion was the new definition of “scientific research”. While the Bill makes this concept wider it is still not clear what can reasonably be described as “scientific”. Does the research need to be for public good? Or peer reviewed?

The Bill also establishes further protections for children by placing an additional statutory duty on the ICO to consider children’s vulnerability regarding data processing. Children’s privacy was also at centre stage at the global DPAs’ assembly in Jersey in October last year (p.26).

*PL&B* is organising a one-day conference in London on 11 March on protecting children’s privacy. As a subscriber benefit, you can get a free place at this event with speakers from the ICO, Lego, K-ID and Ontario’s Information and Privacy Commissioner. You may register your interest now at info@privacylaws.com. Further details to come soon at www.privacylaws.com/children2025.

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.

*Cookies... from p.1*

and Access) Bill will extend these rules to information automatically emitted by terminal equipment. The European Data Protection Board's (EDPB) cookie guidelines take a similarly broad-brush approach.

This expansion is problematic. The analogue principles in the GDPR apply flexibly according to the sensitivity of the personal data; but the cookie rules take a blunt and binary approach. Either the use-case falls within a narrowly defined exception, or GDPR-standard consent is needed.

The main target for these changes is “cookie-like” technologies, such as tracking pixels and browser fingerprinting but there is a risk these changes are applied in an unexpected and unprincipled manner. We dive into the tangled legal and technical issues and consider the problems ahead.

### WHAT ARE THE COOKIE RULES?

The cookie rules originate from the EU ePrivacy Directive. This is *lex specialis* in relation to the GDPR, and contains specific rules on privacy in the electronic communications sector.

Arguably, the impact of the ePrivacy Directive has been just as great as the GDPR, given it is the progenitor of the endless and annoying cookie banners. The cookie rules are, at least, very shortly stated in a single sub-paragraph, Art 5(3): “Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information... inter alia, about the purposes of the processing.”

“This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.”

There are a number of important points about the cookie rules:

- **Scope:** The crux of these rules is its

scope – i.e. is there “storing of information, or the gaining of access to information already stored, in the terminal equipment” of a subscriber or user? The exact meaning of these words is not clear but, as we discuss below, may be expanded dramatically.

- **Consent:** Where the rules apply, they do so in a blunt and binary manner. Consent is required unless one of the narrow exemptions apply. That consent must meet the GDPR standard, which is burdensome and requires an informed and active choice.
- **One-stop-shop:** The one-stop-shop in the GDPR does not apply to the ePrivacy Directive and, in some cases, it is not even enforced by the national Data Protection Authority. This has sometimes been used by national regulators to reformulate an alleged breach of the GDPR as an ePrivacy issue to sidestep the constraints of the one-stop-shop and take direct action against a business with a main establishment in another Member State.

The Art. 5(3) cookie rules clearly apply to http cookies, as the website provider first stores the cookie on the user's browser and then accesses it on subsequent visits. It also applies to spyware programmes designed to access information on an individual's computer without their consent.

The rules' application in other situations – such as browser fingerprinting and tracking pixels – has been controversial given these activities can involve the unilateral transmission of information from the individual's computer, without there necessarily being previous contact with the recipient website.

### EXPANSION IN THE UK – ALL AUTOMATICALLY EMITTED INFORMATION CAUGHT

The UK intends to address this uncertainty by greatly expanding the scope of the “gaining access” concept in the cookie rules. Section 111 of the Data (Use and Access) Bill states that:

*“a reference (however expressed) to storing information, or gaining access to information stored, in the terminal equipment of a subscriber or user includes a reference to instigating the*

*storage or access, and*

*except as otherwise provided, a reference (however expressed) to gaining access to information stored in the terminal equipment of a subscriber or user includes a reference to collecting or monitoring information automatically emitted by the terminal equipment”.*

The second limb of this amendment is most important. This might be intended to apply narrowly to Wi-Fi MAC tracking and similar activities, albeit this is arguably now unnecessary as many phones now randomise MACs<sup>1</sup>. However, it is drafted in extraordinarily wide terms to cover any information that comes out of a computer, phone, smart TV or IoT connected device; to the extent that it is produced “automatically” and “collected” or “monitored”.

The Data (Use and Access) Bill also expands the exceptions to the cookie rules. There will be no need for consent in the following situations:

- **Strictly necessary:** The list of situations in which processing is strictly necessary will expressly include security, fraud detection, detecting faults, authentication and maintaining details of the selections made.
- **Analytics:** The use of analytics cookies will be permitted without consent.
- **Website appearance:** The use of cookies will be permitted where needed to customise the appearance or functions of the service.
- **Emergency assistance:** There is an exception for geolocation to provide emergency assistance.

This expansion appears helpful. However, the exceptions need a detailed and case-by-case review, and some are subject to strict limitations (for example, only applying where the “sole use” of the information is for the identified exemption). The effect of crystallising these exceptions might even narrow them in some cases.

The exceptions also only apply to providers of “information society services”. They therefore might not apply to a broadcast streaming service (if the service is not at the individual request of the recipient), IoT manufacturers and similar.

## EDPB EXPANSION – ALL ONLINE TRACKING REQUIRES CONSENT?

The EDPB *Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive*<sup>2</sup> take a similarly expansive approach to the scope of the cookie rules. However, the Guidelines are not always easy to follow and are an unfortunate mixture of very detailed technology analysis, and loose and inconsistent application of the law. It is also not clear the EDPB has competence to issue guidance on the ePrivacy Directive.

In any event, the guidelines take a broad approach to the concepts of “terminal equipment” and “electronic communications networks”. The guidelines also address the key requirement that there is the “storing of information, or the gaining of access to information already stored”. In relation to this:

- **Passive v active “gaining access”:** The guidelines make it clear that it is not necessary for both “storage” and “access” to take place, such that merely “gaining access” to information falls under the cookie rules. The question is whether that applies to “passive” behaviour (e.g. where the recipient website does nothing to instigate the access) or just where there have been “active” steps? Section 2 suggests this must be active in that “an entity takes steps towards gaining access” to information. However, the examples in section 3 include cases where “passive” behaviour is sufficient, such as simply receiving IP addresses.
- **Storage and access can be by separate people:** The person who stored information on the device and the person to whom the information is sent can be different people. For example, the fact that party A sends the individual the code for a tracking pixel which then leads to a connection to the website of party B, does not take the activity outside the scope of these laws.
- **Storage is broad:** Similarly, the concept of storage is broad and includes placing any information on the relevant terminal equipment, including instructing the terminal equipment to generate and store information. There is no upper or lower time limit on storage so this

would include transitory processing in RAM.

Reading between the lines, it appears the EDPB wants all online tracking to be subject to consent. However, that is not what the law says, even in light of the loose application of technical concepts in the ePrivacy Directive by the CJEU (see *StWL C-102*)<sup>3</sup>.

The EU intended to replace these rules entirely through the proposed EU ePrivacy Regulation. That included significant new detail about the operation of the cookie rules. But the proposed Regulation has made slow progress and may now be shelved.

## CONCEPTUAL PROBLEMS AND EXAMPLES

The expansion of the cookie rules raises a number of difficult conceptual problems.

The main concern is that mere “passive” receipt of information from a terminal device seems to be sufficient to engage these rules. The UK amendments appear to expressly capture “passive” receipt and the EDPB guidelines provide mixed messages (see above). Even if there must be “active” steps to gain access, what does that mean in practice? For example, does the mere fact party B has a website that accepts http connections count as “taking steps”?

This is important as where the information is used for mixed purposes, all of those purposes must fall within an exemption to avoid the need for consent. (“While it is possible to use a cookie for several purposes, such a cookie may only be exempted from consent if all the distinct purposes for which the cookie is used are individually exempted from consent” WP194).

It is worth considering what this could mean in practice:

**IP addresses:** When a user connects to a website, they will provide their IP address so that web pages can be sent back to them. The IP address will very likely be caught by the cookie rules under both the UK amendments (as automatically emitted information) and the EDPB guidelines (see section 3.5). (After all, if IP addresses are not caught, neither

should other information unilaterally sent by the user’s browser to ensure the page is properly displayed, such as screen size, OS, etc. This is, of course, the sort of information used for device fingerprinting.)

The fact that IP addresses are collected is not a problem in relation to the primary use of that information. The IP address will be used to send traffic back to the user. This use is (likely) strictly necessary for service explicitly requested by the user and so that primary use will be exempt from the need for consent.

However, the IP address will typically be logged and then used for a number of different purposes, such as geo-personalisation, website analytics and security. In theory, this means that the website owner should:

- Identify all subsequent use cases for IP addresses.
- Confirm that each of those use cases is subject to an exception. This may not be straightforward. For example, while the UK is proposing to expand the exceptions to include use cases like website analytics, that only applies where the “sole purpose” of the collection is analytics, which would not be the case in relation to the secondary use of IP addresses (Sch 12, para 5(1)(b) of the Bill). In the EU, practices on this point vary. The Spanish Supervisory Authority, for instance, suggests that some first-party analytics may be regarded as strictly necessary for the purposes of the service, particularly when used solely to produce anonymous statistical data, and thus could be exempt from the requirement for user consent.
- Obtain GDPR-standard consent if any of the use cases are not exempt. That would be a significant change to the user experience and impossible to comply with in all cases, for example, at the point the user first visits the website.

For completeness, section 3.5 of the EDPB guidance states that IP addresses will not be caught by these rules where CGNAT is used (i.e. Carrier-grade Network Address Translation where the IP address used by the terminal equipment is changed by the ISP before the traffic enters the public Internet). However, the cookie rules

will still apply in other cases, e.g. where the user has a static IP address or IPv6 addresses<sup>4</sup> are used.

Unless the website “can ensure that the IP address does not originate from the terminal equipment of a user”, the EDPB says the cookie rules apply.

**Business As Usual interactions – Search functionality on a website:** These changes could also affect “business as usual” online interactions that are completely disconnected from cookie technology or online tracking.

For example, consider a website with search functionality – e.g. a box that can be used to insert search terms for content on the site. The primary purpose is to return search results. But imagine those terms are used for a secondary purpose such as creating statistics on the topics that website visitors are interested in.

This involves the website “gaining of access to information already stored, in the terminal equipment” as the letters making up the search term word would need to be stored in the memory of the terminal device for at least a transitory period before being sent to the website. Moreover, this is clearly a situation in which the website “takes steps towards gaining access” as it has chosen to include the search functionality to invite this information.

Accordingly, it appears the search terms used by visitors will fall within the scope of the cookie rules and, unless an exception applies, prior

consent will be needed. Here there is a real risk the exemptions do not apply as the secondary purpose is not necessary for the provision of the service (and will likely not fall within another exception in the new UK rules due to the “sole purpose” requirement, Sch 12, para 5(1)(b)).

#### IN THE REAL WORLD

In practice, it is unlikely that regulators will start using the ePrivacy Directive to fine websites for logging IP addresses or offering search functionality. Enforcement will be targeted at existing areas of concern, such as tracking pixels and browser fingerprinting.

However, it is not beyond the realms of possibility that inventive claimant law firms will use the recast cookie rules to construct new and unexpected class actions. Or that some EU regulators exploit the changes to side-step the one-stop-shop provisions in the GDPR.

The messy legal and technical analysis above also highlights how difficult it will be to get to grips with this extension to the cookie rules and how many different situations are potentially affected. The cookie rules, in theory, create a new “law of everything” regulating almost all Internet interaction.

It would be better if the scope of the cookie rules was clearer and more principled. In the UK at least, the government should either remove section

111(2) from the Data (Use and Access) Bill or limit it to clearly defined “cookie-like” use cases that raise meaningful privacy concerns.

#### AUTHORS

Greg Palmer is a Partner at Linklaters' London office, and Ceyhun Necati Pehlivan is a Co-Leader for the Telecommunications, Media and Technology and IP practice group in the Madrid office.  
Emails: greg.palmer@linklaters.com  
ceyhun.pehlivan@linklaters.com

#### REFERENCES

- 1 support.apple.com/en-gb/102509 MACs (Media Access Controls) are unique hardware addresses that identify devices on a network.
- 2 www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22023-technical-scope-art-53-eprivacy-directive\_en
- 3 *StWL Städtische Werke Lauf a.d. Pegnitz GmbH v eprimo GmbH* curia.europa.eu/juris/liste.jsf?num=C-102/20
- 4 IPv6 operates across a much larger address space so does not need to use GCNAT and part of the IPv6 address is likely to be defined by the terminal equipment.

## ICO comments on Data Bill

The ICO, in its response to the Data (Use and Access) (DUA) Bill has described it as ‘a positive package of reforms’. Some highlights from the ICO’s response include:

“Automated decision-making (ADM) will be possible regardless of the organisation’s lawful basis, as long as suitable safeguards are in place. Most significantly, this will now allow organisations to rely upon legitimate interests for this type of processing. In my view, this strikes a good balance between facilitating the benefits of automation and maintaining additional protection for special category data.”

“The Bill recognises that organisations

are unsure about whether their purpose for processing constitutes a legitimate interest, particularly when it is commercial. The Bill gives more confidence to organisations about when they can rely on the legitimate interests lawful basis. It specifies when the existing legitimate interests lawful basis applies, and in Schedule 4 sets out ‘recognised legitimate interests’ where no balancing test is required. An example is crime prevention and safeguarding, where nervousness about sharing data can cause real harm.”

“It also provides more certainty for organisations to further process personal information. Schedule 5 sets out further

processing purposes that organisations can assume are compatible. Organisations will still need to consider necessity and proportionality. However, in taking this approach, the government has taken on the responsibility for assessing where the balance lies between legitimate interests and people’s rights and freedoms, and whether further processing is compatible at a generic level.”

Technical feedback on several drafting points is included in the annex.

• See [ico.org.uk/about-the-ico/the-data-use-and-access-dua-bill/information-commissioner-s-response-to-the-data-use-and-access-bill/](https://ico.org.uk/about-the-ico/the-data-use-and-access-dua-bill/information-commissioner-s-response-to-the-data-use-and-access-bill/)

*Generative AI... from p.1*

technology-neutral EU General Data Protection Regulation, and its UK equivalent (GDPR). In a recent consultation series on data protection issues posed by the technology (Consultation), the UK's Information Commissioner's Office (ICO) seeks to provide clarity on how it expects organisations leveraging these systems to comply with the GDPR. Perhaps most strikingly, the ICO confirms its position that developers can rely on legitimate interests as a lawful basis to justify the use of web scraping for training generative AI systems, but highlights hurdles that developers must overcome as part of their legitimate interests assessments. The ICO stresses the importance of improving transparency for individuals whose data is processed by generative AI systems, and allowing those individuals to effectively exercise data protection rights. It remains to be seen whether and how industry players will overcome these compliance challenges.

#### BACKGROUND

Building on its continued focus on AI, the ICO launched the Consultation in January 2024 and responded to the input it received on 12 December 2024 (Response). This article examines the key take-aways

the ICO's Consultation largely tackle different data protection issues, but there are areas where their subject matters intersect. While a comprehensive overview of the EDPB Opinion is outside the scope of this article, we have indicated where there is overlap.

#### THE CONSULTATION OUTCOMES Legitimate interests as a lawful basis for web scraping to train generative AI models:

Generative AI models are generally trained using large volumes of data sourced through web scraping. If the scraped data contains personal data, developers must identify a lawful basis under Article 6 of the GDPR, and when capturing special category or "sensitive" personal data, a condition under Article 9 of the GDPR must apply. The Response confirms that personal data (including sensitive personal data) is still processed whether or not such processing is "incidental" or unintentional. Notably, neither the ICO nor the EDPB provide guidance on the use of scraped sensitive data. Given the often indiscriminate nature of web scraping, however, this issue was raised by many respondents to the Consultation, and the ICO is still scrutinising such use.

The Response addresses the appropriate lawful basis, confirming that developers will generally only be able

ICO does not accept the general societal interests of web scraping, or its innovative character, as lone justifications for processing data. Rather, developers should properly define all purposes and demonstrate the benefits in each case. The EDPB, which also addresses this point, provides the following examples of specific purposes which may constitute legitimate interests, provided that the necessity and balance tests are passed: (i) developing the service of a conversational agent to assist users; (ii) developing an AI system to detect fraudulent content or behaviour; and (iii) improving threat detection in an information system.

2. **Necessity test:** Once the purposes are identified, developers must establish that web scraping is the only viable method for achieving them. When launching the Consultation, the ICO's understanding was that generative AI training is only possible through large-scale scraping. However, the ICO learned from the Consultation that there are other methods, such as licensing data from publishers who have collected personal data directly from individuals in a transparent manner. In its Response, the ICO confirmed that developers asserting the necessity of web scraping should explain why they cannot use alternative methods.

3. **Balancing test:** Scraping personal data to train generative AI models must not disproportionately infringe individuals' rights and freedoms. The ICO and the EDPB agree that web scraping poses a high risk to individuals because the processing is "invisible" and not within the individuals' "reasonable expectations".

The ICO considers that most web scrapers fall short of their notification obligations and encourage developers to use innovative mechanisms to provide better transparency and to allow individuals to effectively exercise data protection rights. The ICO also considers that the financial impact on the individual should be factored in to the balancing test; as generative AI may undermine people's livelihoods. This

## The overarching message from the ICO is that current market practices in generative AI are not compliant

from the ICO's opinion on each of the Consultation's five chapters and their implications for the development and deployment of generative AI in the UK.

Shortly after publication of the Response, on 17 December, the European Data Protection Board (EDPB) also issued its eagerly awaited opinion, in response to an Article 64(2) request from the Irish supervisory authority on certain data protection questions related to the processing of personal data in the context of AI models (EDPB Opinion). The EDPB Opinion and

to rely on legitimate interests, as opposed to consent or other bases, when web scraping personal data to train generative AI models. The interest identified by the developer must, however, pass the 'purpose', 'necessity' and 'balancing' tests. The EDPB similarly, in its Opinion, determines that the development (including by web scraping) and deployment of AI models may be based on legitimate interests, offering a detailed overview as to how the three tests may be met.

1. **Purpose test:** Developers must articulate a specific rather than generic interest or "purpose" for processing. The

should be of particular note to the industry.

The ICO considers that developers using web scraping will struggle to pass the balancing test if they fail to implement sufficient protective measures for individuals. Practical guidance from the ICO on what safeguards should consist of is limited. The EDPB Opinion however provides a non-exhaustive and non-prescriptive list of potential risk mitigation measures, including technical pseudonymisation and minimisation techniques, which may serve as a useful reference for organisations subject to the UK GDPR.

Also of relevance is the downstream use of the systems. In some cases, developers may be able to implement controls (e.g. filters to control the system's output) to ensure that its customer's deployment is in line with the legitimate interests identified by the developer. However, developers are not always able to restrict or monitor how a model is used, and the ICO confirms that contractual measures will only be valid to the extent they are effective in practice. For example, the developer will have limited control in an "open-access" system, where the deployer runs its own instance of the model. Developers should pay extra attention to the balancing test when they are unable to mitigate risk in the deployment phase.

from a third-party developing its own application. Additionally, models may be used for different uses downstream.

The ICO confirms that each stage of the lifecycle must have a separate purpose, which is detailed and specific enough so that all relevant parties understand why and how personal data is used. Very broad purposes (e.g. "processing data for the purpose of developing a generative AI model") are not appropriate. As such, collating repositories of web-scraped data, training an AI model and deploying an AI model each require their own explicit and specific purpose.

The Response acknowledges that the open-endedness of downstream deployment may make it challenging for developers of foundation models to be specific about the purpose of processing. However, according to both the ICO and EDPB, the purpose should be articulated as specifically as possible considering the potential use cases and functionality.

**Assessing and communicating the accuracy of training data and model outputs:** The ICO acknowledges that not all generative AI powered systems must be accurate. Accuracy requirements are higher for models intended to generate factual outputs than for systems producing creative or non-factual outputs.

In relation to training datasets, the ICO confirms that the developer

developers should implement controls preventing deployers from using the model for purposes which require accuracy. Particularly in consumer-facing services, additional accuracy safeguards (such as restrictions on user queries and output filters) are deemed particularly important.

**Engineering individual rights into generative AI models:** The ICO confirms that controllers at each stage of the generative AI lifecycle must provide individuals with mechanisms to effectively exercise data protection rights. The ICO stresses the need for data protection by design and default to overcome compliance challenges. For example, common training methods inherently complicate adherence to information rights because the models retain 'imprints' of the training data to learn. As a result, AI systems may generate 'memorised' personal data they were fed during training as outputs. To mitigate this risk, many developers use input and output filters. However, the Response provides that these types of measures are generally not sufficient to comply with erasure requests because the data is not actually removed from the model; developers should ensure they build in effective compliance tools from the outset, or risk their processing being unlawful.

The ICO repeatedly calls on the need for greater transparency – this is not only required by Article 14 of the GDPR, but is also a prerequisite of allowing individuals to exercise rights, and goes to the heart of the legitimate interests balancing test. Neither the ICO nor EDPB come down firmly on when it would be impossible or involve a disproportionate effort for organisations to provide transparency information to individuals and thus be exempt from directly notifying individuals under Article 14 of the GDPR. While the ICO acknowledges in its Consultation that the exemption may be relevant where data is web scraped, it expresses concerns about how such processing is "beyond people's reasonable expectations" and takes the view that just because something is common practice, it does not make the processing expected. In its Response, the ICO stresses that it expects the industry to significantly improve how it informs

---

## Developers should ensure they build in effective compliance tools from the outset, or risk their processing being unlawful.

---

**Identifying clear and specific purposes throughout the generative AI lifecycle:** Personal data may be processed at all stages of the generative AI lifecycle, including training, fine-tuning (e.g. human feedback and benchmarking data) and deployment (e.g. user queries and output), or in the model itself. Different stages may involve processing different types of personal data by different organisations. For example, training a core model will require training data and test data, while adapting the core model may require fine-tuning data

should have a good understanding of how accurate the data is and what it consists of. It should assess the impact of the accuracy of the training data on the outputs and determine whether the statistical accuracy is sufficient for the intended purpose. The developer should curate training data to obtain a sufficient degree of accuracy for the purpose of the model, where possible.

In relation to model outputs, the ICO expects organisations to be transparent about the accuracy limitations of their models, including about potential "hallucinations", and if necessary,

individuals about processing, expecting meaningful solutions “rather than a token gesture”, and that it will not shy away from “taking action when [its] regulatory expectations are ignored”.

Of additional note, the Response addresses the over-reliance of developers on Article 11 of the GDPR. This Article provides that a controller is not required to collect additional information to identify a person to comply with the GDPR, if the purpose for which the controller processes data does not require identification. The ICO does not rule out the application of this exception, but expects organisations to assess on a case-by-case basis whether they are unable to identify an individual and if so, inform that person and offer easy ways for them to provide additional identification information.

**Allocating controllership across the generative AI supply chain:** The ICO recognises that the allocation of responsibility in generative AI supply chains is complex. The roles of “developers” and “deployers” don’t always correspond to the concepts of controllers and processors.

The ICO, in its Response, confirms that developers may act as processors when acting on the instruction of the deployer, but only if the deployer is effectively able to influence the purposes and means of the processing as a controller. This may be the case, for example, in “open-access” models where deployers have the means to fundamentally modify the model.

In contrast, according to the ICO, overarching decisions made by developers (such as decisions about training data, model architecture, risk mitigations and model distribution) often influence how personal data is

processed during deployment, in particular in ‘closed-access’ models. In such cases, where developers retain significant control, the ICO considers that joint controllership between developers and deployers is likely. The ICO argues that, in closed-access models, downstream deployers are not provided with the information they need to control key decision-making as controllers. The EDPB Opinion also acknowledges that joint controllership situations should be considered when assessing the responsibilities of different actors in an AI supply chain.

**IMPLICATIONS FOR DEVELOPING AND DEPLOYING AI IN THE UK**

The ICO’s Consultation and Response provide valuable clarification for developers and deployers of generative AI systems in the UK. In particular, the confirmation that training generative AI systems using web scraping may be based on the legitimate interests of the developer is an important step towards more legal certainty. Further, the ICO has left room for developers to rely on an exemption from providing notice to each individual when web scraping, recognising that doing so could entail disproportionate effort, although it is still unclear what steps developers will need to take to ensure they satisfy the legitimate interests balancing test. The Consultation and Response provide further clarification for organisations on accuracy, purpose limitation and the appropriate role classification in complex generative AI supply chains.

However, the overarching message from the ICO is that current market practices in generative AI are not compliant. In particular, the ICO is concerned about the lack of transparency and the difficulties individuals face

when exercising data protection rights. The regulator relies on industry innovation and expects businesses to develop meaningful solutions, but does not provide clear examples of how compliance can be achieved. Whether stakeholders can rise to this challenge and balance large-scale data processing with robust data protection remains to be seen. Notably, the EDPB Opinion provides more practical examples of safeguards, making it a useful source of inspiration for UK organisations awaiting further guidance from the ICO.

The Consultation and Response reflect the ICO’s current position on generative AI but do not constitute its final stance. The ICO affirms its commitment to further engage with the industry and issue further guidance. Additionally, it will update its positions to reflect future changes to UK data protection law under the upcoming UK Data (Use and Access) Bill and will align them with the forthcoming joint statement on foundation models it is working on with the Competition and Markets Authority. As such, developers and deployers of generative AI in the UK should closely monitor the ICO’s ongoing work in this area.

**AUTHORS**

Josephine Jay and Annabel Loose are Associates at Goodwin.  
Emails: JJay@goodwinlaw.com  
ALoose@goodwinlaw.com

**INFORMATION**

The ICO’s consultation response can be seen at [ico.org.uk/about-the-ico/what-we-do/our-work-on-artificial-intelligence/response-to-the-consultation-series-on-generative-ai/](https://ico.org.uk/about-the-ico/what-we-do/our-work-on-artificial-intelligence/response-to-the-consultation-series-on-generative-ai/)

# Ofcom issues enforcement guidance on Online Safety Act

Ofcom, in charge of enforcing the Online Safety Act 2023, has published guidance on how it will normally approach enforcement under the Act.

If service providers are found non-compliant, Ofcom may issue fines of up to 10% of qualifying worldwide revenue,

or £18 million (whichever is the greater) and require remedial action to be taken.

Service providers have to conduct a risk assessment by the deadline of 16 March 2025. Ofcom says it is ready to take enforcement action if providers do not act promptly.

There are further codes of practice set to be published in the spring.

- See [www.ofcom.org.uk/online-safety/illegal-and-harmful-content/statement-protecting-people-from-illegal-harms-online/](https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/statement-protecting-people-from-illegal-harms-online/)

# New Data Bill will support wider data sharing

Organisations that comply with the UK GDPR should be mostly compliant with the new law, which hopefully will not jeopardise EU adequacy. By **Laura Linkomies**.

The finer details of the Data (Use and Access) Bill<sup>1</sup> (DUAB) were clarified by the Department for Science, Innovation and Technology (DSIT) and the ICO at a recent Briefing<sup>2</sup> organised by *PL&B* together with Linklaters. *Owen Rowland*, Deputy Director at DSIT explained the Bill's overall aims "to enable economic growth, modern digital government and to improve peoples lives". He said that this includes ensuring that the UK retains its EU adequacy decisions, which the European Commission will review in June 2025.

While the new Bill includes changes, for example, to data sharing, legitimate interests, automated decision-making and cookie provisions, *Seema Mistry*, Head of Legislative Reform at the ICO stressed that organisations already complying with UK GDPR will be mostly compliant with the new law. She said that this was a "balanced package of reforms" and while the ICO supports the Bill, the responsibility for drafting lies with DSIT.

Smart data will play a big part in the government's aim for economic growth. The Bill allows for the Secretary of State to issue regulations in this field to enhance use of customer data. "Smart Data schemes", which are the secure sharing of a customer's data upon their request, will be designed with the experience in mind of open banking, a current example of a regime comparable to a Smart Data scheme. The regulations would specify<sup>3</sup>

- Who is required to provide data.
- What data they are required to provide.
- How and when they must provide that data
- How that data is secured and protected, including who authorises access to data.

The Bill enables effective data sharing within the NHS in real time and between different systems, explained

*Oliver Stanley*, Smart Data Legislation Lead, Consumer and Competition Policy, Department for Business and Trade (DBT). It will also clarify when people can use personal data in a research setting.

The government is now working on establishing the National Data Library to make public sector datasets more accessible. It aims to provide greater certainty giving commercial organisations more confidence when processing public sector data, for example when responding to national emergencies.

## SIMILARITIES WITH THE DPDI

*Robin Edwards*, Policy Team Leader, Data Protection Policy, DSIT, explained that the similarities with the previous DPDI Bill include:

- Simplification of scientific research provisions.
- New lawful ground of "recognised legitimate interests".
- Clarification of existing legitimate interests lawful ground (Article 6(1)(f)).
- Clarification of further processing rules.
- Some aspects of the package on subject access requests.
- Changes to Article 22 of UK GDPR on automated decision-making.
- Removal of consent requirements in relation to non-intrusive cookies.
- International transfers of personal data (the UK adequacy test)
- Changes which improve the effectiveness of law enforcement.
- ICO governance changes and modernisation of enforcement powers.

Many unpopular aspects have been omitted. At the time when the DPDI Bill was going through the Parliamentary process, the most lively debate took place on the pure data protection aspects of the Bill. These included changes to the definition of personal

data, compliance obligations on record-keeping, DPIAs, replacing the role of Data Protection Officers with so-called "Senior Responsible Individuals", prior consultation with the ICO, and the appointment of UK representatives. None of these proposals are included in this new Bill. The same applies to giving political parties more freedom to use personal data.

## NEW LEGITIMATE INTEREST GROUNDS

Stemming from experiences during the coronavirus pandemic, the Bill adds a new lawful processing basis for situations to do with national security or emergencies for example where a balancing test would not be needed. Participants at *PL&B's* Briefing thought that the new legitimate grounds could be further expanded.

The DSIT team explained that the Bill tightens regulation-making powers on legitimate interests so that there needs to be a fundamental rights and public interest balancing test. Despite this, the House of Lords has recommended the removal of this power.

The Bill includes examples of types of processing that currently benefit from legitimate interest grounds:

1. processing that is necessary for the purposes of direct marketing;
2. intra-group transmission of personal data (whether relating to clients, employees or other individuals) where that is necessary for internal administrative purposes; and
3. processing that is necessary for the purposes of ensuring the security of network and information systems.

The provisions on direct marketing elevate a GDPR recital into the Bill itself, Rowland said.

The government has also tried to future-proof the Bill; there is also a new power for the Secretary of State to add to the list of special categories of data to ensure that new types of data

are subject to heightened protections (e.g. neuro-data). This is on an ad hoc basis and not something that is planned for at the moment, Rowland said.

### NEW DUTIES FOR ORGANISATIONS AND THE ICO

There will be a new statutory duty for the ICO to consider specific risks to children when carrying out its functions.

The ICO's structure will be modernised along the lines proposed in the DPDI Bill to become a body corporate called the Information Commission. As there will be a number of Commissioners (between three and up to 14), participants expressed concern (in the afternoon meeting without the speakers) that having 14 separate Commissioners would be too many. There were also questions about the process of appointing the Commissioners, as this is not clear in the Bill.

The ICO will be able to require organisations prepare technical reports. An ICO-approved person (internal, external – to be specified) can be asked to report on a specified matter. Linklaters' Partner *Richard Cumbley* observed that there should be a dialogue on who to appoint rather than the ICO dictating. Participants observed that it would be helpful if the technical reports could be produced in-house.

Also, where the Commissioner suspects that a controller or processor has committed or is committing an offence under this Act, the ICO can force an individual (as distinct to a representative of an organisation) to attend an interview.

To enhance accountability and transparency, the ICO must prepare a report on its enforcement actions

### INFORMATION

The Briefing was organised, together with Linklaters and hosted at the law firm, on 25 November 2024.

[www.privacylaws.com/events-gateway/events/uk2024/](http://www.privacylaws.com/events-gateway/events/uk2024/)

As a deliverable following the Briefing, recommendations by the participants were submitted to DSIT, the Department of Business and Trade, the ICO and the members of the House of Lords who spoke in the debate on 19 November.

including information on:

1. the number of investigations begun, continued or completed by the Commissioner during the reporting period;
2. the different types of acts and omissions that were the subject matter of the investigations;
3. the enforcement powers exercised by the Commissioner in the reporting period in connection with the investigations;
4. the duration of investigations that ended in the reporting period; and
5. the different types of outcomes of investigations that ended in that period.

With regard to complaints handling, organisations will be required to deal with any complaints they receive. This is the ICO's preferred method as it will release resources at the office. Individuals may still send their complaint directly to the ICO however, even if the Bill encourages contacting the organisation first.

### SCIENTIFIC RESEARCH

The Bill expands on the current provisions relating to processing for research and statistical purposes. The government's aim is that scientists can

make better use of data.

The new provisions generated many questions and debate amongst Briefing participants. What is understood by scientific research? Does it need to be peer reviewed and in the public interest? When does research stop being scientific? Scientific research should not be the same as market research. Richard Cumbley, Partner, Linklaters, observed that if expanded too far, this is an issue that could negatively affect the UK's EU adequacy.

### TIMETABLE

Rowland explained that the current ministerial team is very experienced and this enabled DSIT to introduce the bill relatively quickly after the general election.

*Sir Chris Bryant MP*, Minister of State for Data Protection and Telecoms, and *Peter Kyle MP*, Secretary of State for Science, Innovation and Technology will drive the Bill, whereas *Baroness Jones of Whitchurch*, Parliamentary Under Secretary of State for the Future of Digital Economy and Online Safety will concentrate more on online safety. Rowland also clarified that DSIT is now the data centre of the government and is an economy and delivery focused department.

The expectation is that the Bill will progress relatively smoothly given that it is largely based on the previous DPDI Bill which was largely agreed on by both the Conservative and Labour parties. In late December the Bill finished the Committee stage and is scheduled to begin the Report stage on 21 and 28 January in the House of Lords.<sup>4</sup> We can expect the Bill to be debated in the House of Commons in January-February, he said. This means

### DMA CAMPAIGNS FOR SOFT OPT-IN FOR CHARITIES

The Data & Marketing Association (DMA), joined with 19 major charities, have urged the government to extend the so-called 'soft opt-in' for email marketing to not-for-profits. "Clause 115 of the previous DPDI Bill extended the 'soft opt-in' for email marketing for charities and other non-commercial organisations. The DMA estimates that extending the soft opt-in to charities would increase annual donations in the UK by £290 million. At present, the DUA Bill proposals remove this provision. The omission of the soft opt-in will prevent

charities from being able to communicate to donors in the same way as businesses can. As representatives of both corporate entities and charitable organisations, it is unclear to the DMA why charities should be at a disadvantage in this regard." Francesca Savage, Deputy Director of Public Income and Engagement, Save the Children UK said: "Supporters are at the heart of everything we do. If Save the Children UK could use the soft opt-in for marketing, it would allow us to connect with supporters more meaningfully by sharing

relevant, timely updates that strengthen our relationship and demonstrate the impact of their contributions. We would use the soft opt-in responsibly, always giving supporters the choice to adjust their preferences at any time. Ultimately, this could transform relationships with supporters and enable us, together, to create lasting change for and with children."

• See [dma.org.uk/article/dma-letter-to-secretary-of-state-peter-kyle-on-behalf-of-the-charity-sector](http://dma.org.uk/article/dma-letter-to-secretary-of-state-peter-kyle-on-behalf-of-the-charity-sector)

Royal Assent could be granted in spring or summer 2025, with further details on commencement date.

The ICO will prepare guidance on areas where there are most changes, and consult appropriately. The ICO's priorities going forward are children's privacy, AI and biometrics, online tracking, cyber security and supporting growth and innovation through use of data, Mistry said.

## REFERENCES

- 1 [bills.parliament.uk/bills/3825](https://bills.parliament.uk/bills/3825)
- 2 [www.privacylaws.com/events-gateway/events/uk2024/](https://www.privacylaws.com/events-gateway/events/uk2024/)
- 3 [www.gov.uk/government/publications/data-use-and-access-bill-factsheets/data-use-and-access-bill-factsheet-growing-the-economy](https://www.gov.uk/government/publications/data-use-and-access-bill-factsheets/data-use-and-access-bill-factsheet-growing-the-economy)
- 4 [bills.parliament.uk/bills/3825/stages/19404](https://bills.parliament.uk/bills/3825/stages/19404)

## DRCF monitors Quantum Technologies

The Digital Regulation Cooperation (DRCF) Forum issued, in November 2024, a paper on quantum technologies in which it outlines the work done by various regulators.

“Given that quantum standards are still in the early stages of development, DRCF member regulators have, to date, adopted an observer role. We recognise that as the standards landscape evolves, there may be opportunities to collaborate more closely and coordinate contributions to ongoing initiatives. This approach aligns with our broader mission to promote responsible innovation while protecting public interests.”

The ICO, in October 2024, published a dedicated futures report exploring the intersection of quantum

technologies and data protection. The report explores possible emerging use cases for quantum technologies, including computing, sensing and imaging that might have data protection implications, and the issues that may arise. The ICO also reflects on its role in the future transition to quantum-secure systems, including next steps that large organisations could take now to prepare.

Organisations should:

- Continue evaluating their risk exposure. This could include identifying high risk information, critical systems and at-risk cryptography;
- Ensure they take evolving international standards and National Cyber Security Centre (NCSC) guidance into account, as required

under the EU Network and Information Systems (NIS) Directive and the UK GDPR; and

- Continue adequately protecting existing information processing, including through basic cyber hygiene.
- See [www.drcf.org.uk/news-and-events/news/new-article—the-quantum-landscape-in-2024-a-year-of-progress-and-drcf-reflections/](https://www.drcf.org.uk/news-and-events/news/new-article—the-quantum-landscape-in-2024-a-year-of-progress-and-drcf-reflections/) and [ico.org.uk/media/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/technology-and-innovation/ico-tech-futures-quantum-technologies-1-0.pdf](https://ico.org.uk/media/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/technology-and-innovation/ico-tech-futures-quantum-technologies-1-0.pdf)



### Data opportunities in Ireland: PL&B's Conference with new Data Protection Commissioner Dr Des Hogan

6 February 2025

Host: McCann FitzGerald, Dublin, Ireland

Come and meet Dr Des Hogan and Deputy Data Protection Commissioners, Heads of regulators for Telecoms, Media, and Competition and Consumer Protection. Other speakers are from the European Data Protection Board, Anthropic, OpenAI, Autodesk, Workday and Vodafone and

leading data protection lawyers from Dublin and Brussels.

**Why you need to attend:** Ireland issues a large proportion of fines in Europe, and contributes to important interpretations of privacy laws.

Early bird discount period ends on 17 January.

See the programme and register at [www.privacylaws.com/ireland2025](https://www.privacylaws.com/ireland2025)

### What is right for children and their data? PL&B conference on Children's privacy

11 March 2025

Host: A&O Shearman, London, UK  
Further details to come soon at [www.privacylaws.com/children2025](https://www.privacylaws.com/children2025)

### CPDP.ai 2025: The world is watching

21-23 May 2025

Brussels, Belgium

See [www.cpdpcferences.org/](https://www.cpdpcferences.org/)

### The Good, The Bad and The Good Enough: PL&B's 38th International Conference

7-9 July 2025

St John's College, Cambridge, UK

See [www.privacylaws.com/plb2025](https://www.privacylaws.com/plb2025) for 24 sessions and to register with Very Early Bird fees by 31 January 2025.

# Data (Use and Access) Bill: Automated decision-making in the spotlight

Proposals grant controllers increased flexibility for automated decision-making, provided suitable safeguards are implemented. By **Fiona Maclean, Gail Crawford, Amy Smyth** and **Lorenzo Meusburger** of Latham & Watkins.

On 23 October 2024, the UK government introduced the Data (Use and Access) Bill (the Bill) to Parliament, marking a significant step in the evolution of the country's data protection landscape. It follows previous reform attempts that lapsed after the July 2024 government change. The proposed legislation aims to reform various aspects of UK data protection law while also addressing broader initiatives related to data access and digital identity. Among its many provisions (138 Clauses, 16 Schedules and 251 pages to be precise), the Bill outlines notable changes in the realm of automated decision-making. In this article, we will delve deeper into the Bill, with a particular focus on the legislative changes surrounding automated decision-making, exploring their potential implications and the future they may herald for individuals and organisations alike.

## OVERVIEW OF THE BILL

Compared to the previous government's flagship data protection reform initiative (the Data Protection and Digital Information (No. 2) Bill), the current Bill proposes slightly less extensive changes to the current data protection regime, but retains a number of the earlier proposals, such as those on legitimate interests, automated decision-making, and ICO reforms. Key proposals include:

1. Enhanced access frameworks for customer and business data, which will make it more efficient for both industry and the public to use personal information in beneficial ways and which mirror certain provisions in the EU's Data Act;
2. A framework for individual ID verification services;

3. Targeted amendments to UK data protection law, maintaining the UK GDPR framework but with changes including:

- a) a specific list of "recognised legitimate interests", which are exempt from the UK GDPR's balancing test for the purposes of the legitimate interest legal basis;
- b) a relaxation of the current restrictions on automated decision-making;
- c) a risk-based approach to adequacy decisions (rather than the EU's equivalence-based approach), which will be applied by the Secretary of State, and which will require third countries to maintain protections "not materially lower" than those in the UK;
- d) a less restrictive approach to cookies and tracking technologies, in particular allowing certain non-intrusive cookies and similar technologies without user consent and enabling consent via browser tools to reduce the use of consent banners. Additionally, it proposes increasing fines for breaches of the cookie-related rules in the Privacy and Electronic Communications Regulations 2003 to UK GDPR levels, i.e. up to £17.5 million or 4% of global turnover; and

4. Transitioning the ICO to a new corporate structure, renamed the 'Information Commission'.

The Bill is currently going through the legislative stages and is subject to further debate and amendment. It has passed its first and second readings in the House of Lords as well as the Committee stage, and at the time of writing was at the Report stage.

## WHAT ARE THE PROPOSED CHANGES TO ADM?

Currently, under Article 22(1) of the UK GDPR, individuals have the right to not be subjected to decisions made solely by automated processes, including profiling, that have legal effects or similarly affect the individual, unless (i) where such processing is necessary for entering into, or the performance of, a contract between a controller and a data subject, (ii) where such activity is required or authorised by law<sup>1</sup>, or (iii) where a data subject has provided explicit consent (Article 22(2)).

Clause 80 of the Bill introduces notable changes to the existing framework under Article 22 UK GDPR. Specifically, the Bill substitutes Article 22 with new Articles 22A-D whereby unrestricted automated decision-making is not limited to those three circumstances described above. In essence, the Bill's changes mean that, apart from cases using special category data, automated decision-making, which results in a legal or similarly significant effect, will no longer be restricted (and permitted only under those three lawful grounds described above), but instead, such processing will be permissible regardless of the lawful basis relied on, as long as suitable safeguards are in place. The ICO, in its commentary on the Bill, notes "[m]ost significantly, this will now allow organisations to rely upon legitimate interests for this type of processing".<sup>2</sup>

The Bill's aim with these changes is to provide more flexibility to businesses while retaining appropriate assurances and safeguards for data subjects (which are discussed in more detail below). In the ICO's response to the Bill, the Information Commissioner welcomed the proposed changes

introduced by the Bill with respect to Article 22 UK GDPR, and stated: “In my view, this strikes a good balance between facilitating the benefits of automation and maintaining additional protection for special category data.”<sup>3</sup>

### DOES THE BILL ALTER THE DEFINITION OF ADM?

The proposed new Article 22A of the UK GDPR defines automated decision-making and retains the existing elements under Article 22 UK GDPR, although it supplements it with the element of “meaningful human involvement”. Specifically, it states that “a decision is based solely on automated processing if there is no meaningful human involvement in the taking of the decision, and a decision is significant, in relation to a data subject, if (i) it produces a legal effect for the data subject, or (ii) it has a similarly significant effect for the data subject” (Article 22A(1)).<sup>4</sup> Articles 22D(1) and D(2) confer powers to the Secretary of State to clarify what qualifies as (i) meaningful human involvement, and (ii) a significant decision with similarly significant effect for the data subject. The explanatory notes to the Bill state that these powers “will allow the Secretary of State to determine when meaningful involvement can be said to have taken place in light of constantly emerging technologies, as well as changing societal expectations of what constitutes a significant decision in a data protection context.”

Until such regulations have been published by the Secretary of State, organisations may want to consider existing guidance which is helpful in respect of certain interpretive matters. For example:

- According to the ICO’s guidance on the term “solely”<sup>5</sup>, if a human inputs the data or merely applies the decision taken by the machine, the process would still be considered a solely automated decision made by an automated system. However, if a human actively evaluates and interprets the automated decision before it is applied to an individual, the process would not be considered solely automated, so long as such action is more than a mere token gesture and the human reviewer has real discretion to alter the machine’s

outcome. One could reasonably presume that the new element of “meaningful human involvement” will rely and build on this existing guidance.

- A decision with a legal effect impacts a person’s legal status or rights, such as eligibility for a legal benefit like housing assistance. A decision with a similarly significant effect has a comparable impact on an individual’s circumstances, behaviour, or choices. The assessment here should be contextual, meaning that similarly significant effects may arise with respect to the treatment of vulnerable individuals (like children), but may not arise in other circumstances. Examples include automatic denial of online credit, e-recruitment without human involvement, discrimination and exclusion of individuals, and relevant factors to consider include the impact on a person’s financial situation, health, reputation, employment opportunities, behaviour, or choices.

In addition, note that under the new Article 22A(2), “when considering whether there is meaningful human involvement in the taking of a decision, a person must consider, among other things, the extent to which the decision is reached by means of profiling.” It is currently unclear what the profiling element (i.e. that controllers need to consider the extent to which the decision is reached based on profiling) means in practice, and what impact such element has on a controller’s assessment whether there is meaningful human involvement. Neither the explanatory comments to the Bill, nor the ICO’s technical drafting comments provide additional clarity.

In conclusion, Article 22A does not propose any radical departure or material changes to the meaning of automated decisions and the proposed changes mostly bring the law in line with what existing ICO guidance has already stated, although there is no doubt that the publication of supplementary regulations by the Secretary of State under Article 22D(1) and D(2) (as well as regulatory guidance on the profiling element described above) will be welcomed by individuals and businesses for additional certainty.

### WHAT ARE THE LIMITATIONS ON THE NEW ADM PROVISIONS?

The proposed language for the new Article 22B(1) makes clear that a “significant decision” (i.e. one that produces legal effects or in a similar way significantly affects the data subject) may not be taken by a controller on the basis of automated decision-making, if it is entirely or partly based on the processing of special categories of data (as set out Article 9(1) UK GDPR).<sup>6</sup> In such case, lawful processing requires controllers to meet one of the following two conditions:

1. The controller obtains the data subject’s explicit consent; or
2. The processing is necessary for reasons of substantial public interest (per Article 9(2)(g) UK GDPR) and the decision is either:
  - a) necessary for entering into, or performance of, a contract between the data subject and a data controller; or
  - b) required or authorised by law.

A further notable restriction introduced by the Bill is that where processing of, or on behalf of, the decision-maker is based on new Article 6(1)(ea) of the UK GDPR (i.e. processing is necessary for the purpose of a recognised legitimate interest), then a significant decision solely based on automated processing may not be taken.<sup>7</sup>

### IMPLICATIONS FOR CONTROLLERS’ USE OF AI SYSTEMS

The Bill’s proposed changes will simplify a number of processing operations that may have previously required careful planning and comprehensive risk assessments in order to comply with Article 22 UK GDPR. For example, in the realm of AI processing, the proposed relaxations will be beneficial to businesses who want to deploy AI tools on datasets containing non-special categories of personal data for automated decision-making. This aligns with the UK’s general principles-based approach to AI regulation, which is currently relatively light-touch and seeks to facilitate innovation by affording businesses with more flexibility around automated decision-making (in particular when deciding on the extent of human review within the automated decision-making process). Although a

limitation on the processing of special category data for automated decision-making persists, the new framework encourages responsible innovation, as long as certain safeguards, such as transparency and review processes, as explained below, are upheld by the controller. Below are two use cases where the legislative proposal may benefit controllers:

- **In HR and recruitment**, AI tools can streamline decisions, such as on the calculation of wages, bonuses, or decisions regarding access to employment benefits, dismissals, etc. as well as assist with the initial screening of job applications by filtering candidates based on predefined criteria. Under the current requirements, there is a risk that the aforementioned use cases could fall within the scope of Article 22 UK GDPR (depending on the particular circumstances) and controllers may therefore find themselves restricted with what tools they can implement to make decisions about individuals, as an appropriate legal basis may not be available. The proposed changes mean that controllers will have more flexibility with respect to the legal bases they deem most appropriate to the processing (unless the processing includes special categories of personal data), though they will still need to implement the proposed safeguards outlined below (including on the provision of human intervention on the data subject's request), and comply with other generally applicable provisions of the UK GDPR for the processing of personal data. In practice, controllers should review any AI-generated outcomes that may materially affect employees and job candidates to ensure that no individual is disadvantaged, for example, as a result of algorithmic biases.
- **In the financial services sector**, automated systems are often used for credit scoring and loan approvals. Using such automated systems, for example for credit scoring to determine loan approvals, will likely fall within the scope of Article 22. However, under the

proposed changes in the new framework, such use case would no longer be restricted to the three specific legal bases permitted under Article 22(2) (unless controllers use special categories of personal data) and businesses could undertake automated decision-making using AI to process applications more swiftly by relying on a legitimate interest legal basis (depending on the specific circumstances). Controllers would, however, still need to comply with other applicable GDPR provisions for such processing (including a balancing test), and implement appropriate safeguards (as detailed below), including reviewing mechanisms for identifying cases that fall outside standard parameters (e.g. with respect of vulnerable individuals), to ensure that applicants are not, for example, unfairly denied credit.

#### TO WHAT EXTENT DOES THE BILL DIVERGE FROM THE EU GDPR?

The proposed UK approach to automated decision-making under the Bill appears to somewhat diverge from the expansive interpretation of Article 22 EU GDPR, as seen in the recent SCHUFA decision by the Court of Justice of the EU (C-634/21) (*PL&B International Report*, April 2024, p.1). In *SCHUFA*, the court applied Article 22 strictly, potentially extending its restrictions to data processing activities that precede the actual decision if the decision heavily relies on such processing.

This interpretation could, for example, bring a wide range of AI data analytics tools within the scope of Article 22 EU GDPR, impacting how businesses in the EU approach automated decision-making. In contrast, the UK's proposed framework under the Bill offers more flexibility by narrowing the scope of Article 22 UK GDPR.

This divergence could lead to notable differences in how automated decision-making is regulated and practised between the UK and EU, depending on how national courts and supervisory authorities choose to enforce the *SCHUFA* ruling. Businesses operating across both jurisdictions will need to navigate these differences carefully to ensure compliance.

#### WHAT SAFEGUARDS SHOULD CONTROLLERS ADOPT FOR ADM?

The safeguards proposed by the Bill at Article 22C replace the current provisions at Article 22(3) and Article 22(3A) of the UK GDPR and s.14 of the Data Protection Act 2018. Any processing of personal data (including special category of data) will need to implement certain safeguards under the proposed new Article 22C, which provides that where a significant decision is taken by or on behalf of the controller in relation to a data subject and such decision is "(a) based entirely or partly on personal data, and (b) based solely on automated processing, the controller must ensure that safeguards for the data subject's rights, freedoms and legitimate interests are in place."

These safeguards must comply with any future regulations issued by the Secretary of State on automated decision-making, and must also consist of or include measures which:

- a) provide the data subject with information about the significant decisions taken on the basis of automated means and associated personal data processing;
- b) enable the data subject to make representations about such decisions;
- c) enable the data subject to obtain human intervention on the part of the controller in relation to such decisions; and
- d) enable the data subject to contest such decisions.

#### PRACTICAL IMPLEMENTATION CHECKLIST

To implement the safeguards outlined in the proposed new Article 22C, controllers should focus on (i) transparency, (ii) human oversight, and (iii) effective communication. This involves:

1. Creating clear channels to inform data subjects about automated decision-making processes, including revising sufficiency of disclosures in existing privacy notices and update them, if necessary, to ensure they explain the personal data used and the logic behind decisions.
2. Establishing a dedicated team or allocating specific responsibilities to employees for oversight ensures that human intervention is available when needed, allowing for

- meaningful human evaluation and the ability to alter outcomes if necessary.
3. Additionally, controllers should consider providing simple means in apps and sites for data subjects, possibly within existing account settings and data management tools, to submit feedback and request human intervention on any automated decision-making processes to engage with any decisions that may affect them.
  4. In general, controllers should also consider regular audits and reviews of automated systems to identify potential biases or errors within the automated decision-making systems as well as the processing of any special category of data (for example on an incidental basis) to ensure compliance, fairness and accuracy.
  5. Training staff on the legal and ethical implications of automated decision-making reinforces a culture of responsibility, while comprehensive policies and procedures of processes and decisions support transparency and accountability.
  6. Concrete steps for controllers include documenting:
    - a) the steps they have taken with regard to the above and the safeguards that have been implemented;

- b) the data used, decision criteria, and instances of human intervention within the automated decision-making process; and
- c) any changes made to decisions following data subject representations or human review.

## CONCLUSION

There is no doubt that the Bill presents both challenges and opportunities for businesses. By embracing the flexibility offered by the new framework, companies can innovate responsibly, leveraging AI and automated decision-making to enhance efficiency and competitiveness. However, this must be balanced with a commitment to transparency and accountability, ensuring that the rights and interests of individuals are safeguarded. The Bill's emphasis on meaningful human intervention and robust safeguards underscores the importance of integrating human oversight into automated processes. For businesses, this means not only complying with legal requirements but also fostering trust *vis-a-vis* their data subjects.

For the moment, the Bill's reception by trade unionists, civil society groups, and academics has been rather negative, as seen in an open letter dated 6 December 2024<sup>8</sup> to Technology Minister, the Rt Hon. Peter Kyle,

urging amendments to the Bill to change its proposals on automated decision-making. The campaigners caution that deviating from existing data protection laws could strip individuals of their right to avoid "life-changing decisions made solely by machines." Signatories, including Amnesty International, Privacy International, and the Open Rights Group, advocate for revisions to the Data (Use and Access) Bill to maintain the accountability necessary for public confidence in AI technology and decisions solely made by machines.

## AUTHORS

Fiona Maclean and Gail Crawford are Partners at Latham & Watkins, Amy Smyth is a Knowledge Management Counsel, and Lorenzo Meusburger is an Associate at the same firm.  
Emails: [fiona.macleam@lw.com](mailto:fiona.macleam@lw.com)  
[gail.crawford@lw.com](mailto:gail.crawford@lw.com)  
[amy.smyth@lw.com](mailto:amy.smyth@lw.com)  
[lorenzo.meusburger@lw.com](mailto:lorenzo.meusburger@lw.com)

## REFERENCES

- 1 Note that in the UK GDPR, this exception refers to "qualifying significant decision" for the purposes of Section 14 of the 2018 Act). "Qualifying significant decision" is a decision taken by the controller that (i) produces legal effects or similarly significantly affects the data subject, (ii) is "required or authorised by law", and (iii) which does not fall within Article 22(2)(a) or (c) of the UK GDPR (i.e. decisions necessary to a contract or made with the data subject's consent). (Section 14(3) Data Protection Act 2018).
- 2 Available at: [ico.org.uk/about-the-ico/the-data-use-and-access-dua-bill/information-commissioner-s-response-to-the-data-use-and-access-bill/](https://ico.org.uk/about-the-ico/the-data-use-and-access-dua-bill/information-commissioner-s-response-to-the-data-use-and-access-bill/)
- 3 Available at: [ico.org.uk/about-the-ico/the-data-use-and-access-dua-bill/information-commissioner-s-response-to-the-data-use-and-access-bill/](https://ico.org.uk/about-the-ico/the-data-use-and-access-dua-bill/information-commissioner-s-response-to-the-data-use-and-access-bill/)
- 4 Note that the Bill seems to propose a slightly different approach for intelligence services' processing for automated decision-making under Part 4 of the Data Protection Act 2018. The Bill's Article 22D notes in this regard that "a decision is based on entirely automated processing if the decision-making process does not include an opportunity for a human being to accept, reject or influence the decision." According to the ICO's technical drafting comments at Annex One of the ICO's response to the proposed Bill, the aforementioned language resulted in a point of criticism as a result of the uncertainty with respect to what "opportunity" means. Specifically, the ICO notes that its understanding "is that the government's intention is that a mere 'opportunity' for human involvement in a decision will not be sufficient to take a decision outside of the scope of "a decision based on entirely automated processing". [Intelligence Services] Organisations would have to exercise this opportunity to have this effect. It would be useful to make the intent clear in the drafting or the explanatory notes."
- 5 Available at: [ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/automated-decision-making-and-profiling/what-does-the-uk-gdpr-say-about-automated-decision-making-and-profiling/](https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/automated-decision-making-and-profiling/what-does-the-uk-gdpr-say-about-automated-decision-making-and-profiling/)
- 6 Special categories of data include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. (Article 9(1) UK GDPR)
- 7 Article 22B(4) Data (Use and Access) Bill
- 8 Available at: [www.openrightsgroup.org/press-releases/letter-to-peter-kyle-keep-our-right-not-to-be-subjected-to-decisions-based-solely-on-ai/](https://www.openrightsgroup.org/press-releases/letter-to-peter-kyle-keep-our-right-not-to-be-subjected-to-decisions-based-solely-on-ai/)

# The new UK approach: Making international transfers easier?

By Rachael Annear, Joseph Mason, Adam Gillert and Rhea Dennis of Freshfields.

On 23 October 2024, the UK government introduced the Data (Use and Access) Bill to Parliament (the DUAB).

One area of change is the international transfer regime, where the DUAB may make it easier for businesses to transfer personal data outside of the UK. While expected guidance from the newly structured Information Commission, and case law, will determine the full extent of these changes, this article summarises what businesses need to know now about the new approach.

## CURRENT APPROACH TO TRANSFERS UNDER THE UK GDPR

Controllers can currently transfer personal data outside of the UK only if:

1. the third country is covered by a UK adequacy decision; or
2. the transfer is covered by appropriate safeguards, such as the entry into an International Data Transfer Agreement.

Transfers can also be made in limited circumstances when an exception applies.

If the UK government decides that a third country's data protection regime has adequate protections, also known as an adequacy decision, data can be transferred there without appropriate safeguards. Currently, when deciding if a third country is adequate for the purposes of an international transfer, the UK government must have regard to consideration of, among other factors, the impact on human rights and fundamental freedoms and the existence of supervisory institutions in that country.

When relying on appropriate safeguards, UK controllers must conduct transfer risk assessments. One element of those risk assessments is ensuring that, post-transfer, the personal data will be protected in a way that is "essentially equivalent" to the level of protection under the UK GDPR. This standard arose from the *Schrems II* decision.

## A NEW THRESHOLD FOR ASSESSING TRANSFERS

The DUAB introduces a new "data protection test" into the UK's international transfers regime. This replaces the previous test and must be applied in the following two primary circumstances:

- when the UK government is making an adequacy decision about the data protection regime of a third country; and
- when a business is undertaking a transfer risk assessment and must assess the risks of the data protection regime of the third country it is transferring data to.

In both circumstances, the DUAB requires the replacement data protection test to be applied. This test will be met when the standard of protection provided for data subjects in the third country is "not materially lower" than the standard of the protection provided under the UK GDPR.

It is not yet clear how "not materially lower" differs from "essentially equivalent" under the current regime. It will be up to the Information Commission and the UK courts to provide guidance on this point. The intention of the DUAB, however, appears to be to introduce a different, likely slightly lower, standard for making international transfers under the UK GDPR than currently exists under the EU GDPR.

The Explanatory Notes to the DUAB state that, making an assessment of the data protection test, the Secretary of State should recognise that "other countries' data protection regimes will not be identical to the UK's in form and differences may exist given the cultural context of privacy". The Secretary of State must, "in a holistic and contextual manner, decide whether or not the overall standard of protection is lower than the UK's standard in a way which is material."

The effect of this new test is likely to make it easier for both the UK

government to designate certain third countries as adequate, and for businesses to carry out risk assessments when relying on appropriate safeguards. These changes may, taken together, make it easier for businesses to transfer personal data outside of the UK.

A business's existing transfer mechanism can still be compliant and provide appropriate protection if:

- it was entered into before the commencement of DUAB; and
- it otherwise satisfies the requirements of the UK GDPR international transfer regime prior to the commencement of the DUAB.

A business will need to apply the new data protection test when it enters into a new transfer mechanism after commencement of the DUAB.

## INTRODUCTION OF TRANSFER BLACKLISTS

The DUAB also allows the UK government to place certain countries on a transfer "blacklist", banning businesses and other organisations from transferring personal data there, where the restriction is in the public interest. This approach differs from many other jurisdictions (including the EU), and will allow the UK government to wholesale restrict transfers of personal data to certain countries.

## IMPLICATIONS AND NEXT STEPS CHECKLIST

Businesses should be aware of the following before the DUAB's entry into force:

1. If you have international transfer mechanisms in place already, you do not need to update this as a result of DUAB (assuming they are already compliant with the UK GDPR).
2. When you enter into new transfer mechanisms post-commencement of the DUAB, you will need to apply the new transfer mechanism at that stage.
3. It is possible that the UK government could use the DUAB to designate as adequate a greater number

of third countries, making it easier for businesses to transfer personal data without the need for additional safeguards.

4. Where you are conducting transfer risk assessments, you should consider whether your processes will need to be updated to reflect the new “data protection test”.
5. Businesses should proactively

monitor additions to the “blacklist”. When jurisdictions are added to the “blacklist”, consider what impact that will have on your business if you are transferring personal data to those jurisdictions and what mitigations may need to be implemented.

#### AUTHORS

Rachael Annear is a Partner, Joseph Mason an Associate, Adam Gillert a Global Data Knowledge Lawyer, and Rhea Dennis a Trainee Associate at Freshfields.

Emails: [Rachael.Annear@Freshfields.com](mailto:Rachael.Annear@Freshfields.com)  
[Joseph.Mason@Freshfields.com](mailto:Joseph.Mason@Freshfields.com)  
[Adam.Gillert@Freshfields.com](mailto:Adam.Gillert@Freshfields.com)  
[Rhea.Dennis@Freshfields.com](mailto:Rhea.Dennis@Freshfields.com)

# A focus on the digital Identity provisions in the DUA Bill

Creating a trusted framework means that digital verification service providers must adhere to privacy rules. By **Nicola Fulford** of Hogan Lovells.

Digital identities are key in an online economy, and verifying identity is nothing new. It is a challenge that online banking apps, government departments and services requiring age verification have been grappling with for a long time, and was brought into even sharper focus during the Covid pandemic when there were challenges with proving identity physically. At its heart, of course, is the accurate processing of personal data.

The much anticipated Data (Use and Access) or DUA Bill was introduced to Parliament on 23 October,

people’s lives easier.

This article discusses the draft proposals with respect to the planned certification framework for digital identity verification.

There were provisions in the previous DPDI Bill on digital identity verification, so this is not entirely new territory, indeed much in the new Bill is very familiar. There have also been calls for a scheme for online identity verification for years now, for example, it was discussed in the Kalifa review of FinTech published in 2021. It’s important to note that the proposal is a voluntary scheme, and not

individuals, such as in assisting age verification checks, pre-employment checks or moving house, and will have a broad applicability across a range of sectors.

A digital identity is a digital representation of a person or things about them. It lets people prove these things without presenting physical documents and all the information they contain. According to the Bill, the new verification services will ascertain a fact about the individual from information provided otherwise than by the individual, and confirm to another person that the fact has been ascertained.

The proposal is a voluntary scheme, and not aiming to introduce national digital identity cards.

#### TRUST FRAMEWORK AT THE HEART OF THE SCHEME

The Bill does not set out all the details of how this will work. Instead, it confers a duty on the Secretary of State to prepare a framework for establishing digital verification services. Unlike in the DPDI Bill, the Information Commissioner will be consulted in relation to secondary regulations as to how this framework will be implemented in practice, which is likely to be welcomed by privacy practitioners. New additions to the Bill compared with the DPDI Bill also include a right for the Secretary of State to refuse certification to organisations on national security grounds, a right that at this stage would not seem controversial.

had a second reading in the House of Lords in November, and the Committee Stage finished on 18 December. Overall, the new DUA Bill is about the better use of data, including smart data schemes, targeted data protection reforms and introducing a certification framework for digital identity verification. The government claims the Bill will use the power of data to help grow the economy through innovation, improve public services through secure and effective use of data, and make

aiming to introduce national digital identity cards.

The DUA Bill will support the creation and adoption of trusted digital verification services from certified providers in the UK, with the aim of then enabling individuals and businesses to embrace secure digital identities. This would replace existing processes of having to provide physical copies, for example of passports or driving licences.

The government says this will help

It will not be mandatory to adopt

the framework, but organisations can apply for certification as a provider. Organisations that do comply with the framework will be added to a register of trusted organisations, and those who have been certified will be given a ‘trust mark’. It is hoped that the use of a trust mark will increase individuals’ confidence with whom they share their personal data, and that organisations displaying the trust mark will process personal data to a stringent set of standards.

The framework will be overseen by the Office for Digital Identities and Attributes (OfDIA), part of DSIT.

Part 2 of the Bill sets out provisions to secure the reliability of digital verification services by means of a number of elements:

- **Trust Framework:** A trust framework setting out rules for the provision of digital verification services (there may be different rules for different verification services); together with
- **Supplementary codes.**
- **A Register:** A requirement to establish and maintain a register of certified organisations providing digital verification services (DVS).
- **Information Gateway:** Including powers enabling public authorities to share information in relation to an individual with an organisation registered in the DVS register, provided the individual has made a request to provide the information.

- A requirement for the Secretary of State to publish a **Code of Practice** regarding disclosing information which should be consistent with the ICO’s statutory data sharing code.
- **A Trust mark** for use by certified organisations: a power for the Secretary of State to designate trust marks to organisations registered to provide digital verification services i.e. those who have complied with the trust framework.

#### PRIVACY SAFEGUARDS

The key risks to be considered and mitigated, in line with existing data protection and equality laws, are as follows:

- **Privacy** – individuals and businesses who use the services will need trust in the data sharing; to enable this trust, there must be transparency, and control for individuals over their data.
- **Inclusiveness** – it must not exclude already marginalised groups.
- **Security** – it is obviously vital that the data is kept secure, and only shared with permission.

A further issue, which looks likely to be left to organisations to determine through contractual arrangements (or scheme level terms) rather than being set by the government, is liability. This has proved to be a stumbling block in the past. Interoperability will also be a challenge, likely helped by compliance with standards.

Interestingly, DSIT has set out a number of rules that certified providers will have to comply with, including:

- Not “profiling” users for third party marketing purposes.
- Not creating large datasets that could risk revealing sensitive data about users.
- Explicitly confirming that users understand how their data is being shared, whenever this happens.

Given the business models of some potential providers, this is an area to watch.

It seems that the DUA Bill provisions on digital identities have been broadly welcomed. As the proposals were not one of the controversial elements in the previous DPDI Bill, it looks likely that this aspect of the Bill will proceed largely as drafted. While still in its early stages, a smooth trajectory is expected through Parliament at a fairly rapid pace. Both private and public sector entities will therefore be keen to see further details of the trust framework from OfDIA, so that we can assess how this will work in practice.

#### AUTHOR

Nicola Fulford is a Partner at Hogan Lovells.  
Email: [nicola.fulford@hoganlovells.com](mailto:nicola.fulford@hoganlovells.com)

## Court of Appeal rejects appeal against ICO’s Monetary Penalty Notice

The ICO says it welcomes the Court of Appeal’s dismissal of an appeal by Doorstep Dispensaree Limited, issued against the ICO’s Monetary Penalty Notice (MPN) of December 2019.

Doorstep Dispensaree’s arguments were rejected by the Court which said that the burden of proof in an appeal lies with the appellant. Subsequent tribunals and appeal courts are not required to start considering an appeal with a “blank sheet of paper”, essentially ignoring the MPN.

The company’s successful appeal to the First Tier Tribunal saw the fine reduced to £92,000, but it was unable to convince the Upper Tier Tribunal to overturn the fine completely (*PL&B UK Report*, September 2023, p. 11).

Information Commissioner John Edwards said: “I welcome the Court of Appeal’s judgment in this case as it provides clarity for future appeals. We defended our position robustly and are pleased that the Court has agreed with our findings.”

“The case raised issues of considerable importance for ongoing and future appeals of penalties issued, and the Commissioner is grateful to the Court for clarifying the points of law.”

- See [ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/12/court-of-appeal-rejects-appeal-against-uk-information-commissioner-s-monetary-penalty-notice/](https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/12/court-of-appeal-rejects-appeal-against-uk-information-commissioner-s-monetary-penalty-notice/)

# Dame Wendy Hall: UK should not follow EU's approach on AI

Dame Wendy Hall is optimistic that the UK's sectoral approach to AI will be the correct way to proceed but she envisages that we will also see regulation. **Laura Linkomies** reports.

**D**ame Wendy Hall, DBE, FRS, FREng, Regius Professor of Computer Science at the University of Southampton, is well placed to evaluate the UK's plans for AI. Not only was she a pioneer of multimedia and hypermedia in the years before the World Wide Web, but she was also co-Chair of the previous government's AI Review published in October 2017, and a member of the AI Council. She advises the UK government and many other governments and companies around the world. In 2023, Hall was appointed to the United Nations' high-level advisory body on artificial intelligence.

At the time of my interview, at the end of October, the government had just published the Data (Use and Access) Bill<sup>1</sup>, but we have yet to see a general AI Bill. The King's speech in July 2024 indicated that only the most powerful artificial intelligence models will be regulated, overseen by a new Regulatory Innovation Office<sup>2</sup>. Hall implied, however, that the UK is not misguided to have a more narrowly focused approach different from the EU, and that there is more to come.

"We want to be seen to be doing this properly in the UK ... but I think in the EU, the AI Act was adopted too early. We do not know yet what we are trying to regulate. The EU AI Act does possibly stop innovation – some companies are already saying they do not want to operate in the EU due to the AI Act. I do think it is too restrictive – but we can now learn from this experiment in the UK. It is possible that the current government will rework the Conservative government's AI White Paper and turn that into a regulation. There would also be a coordinator for that regulation – the lack of one was the main criticism of the White Paper."

Hall thought that the AI Safety Institute will remain, and that AI will be regulated through it – the Institute could be the cornerstone of the new Bill.

"I think the intention of the White Paper, to use existing agencies, and not to undo what we already have in place is right. I do not think we will have a separate AI agency – that is the current thinking. Data and AI should not be separate – you cannot do one without the other. The overall authority may lie in something like the AI Safety Institute, but it will cooperate with the Information Commissioner's Office (ICO), the Competition and Markets Authority (CMA) and the other agencies as a collective. To me that seems like a good approach; we have very good agencies in the UK."

The ICO has been active in issuing AI guidance and says that GDPR principles apply. Asked about the ICO's action on LinkedIn and Meta to steer them away from utilising their users' personal data to train generative AI, Hall commented: "It is one of the ways to regulate. We do need an authority that looks after people's personal data used by AI – and the ICO is one of the agencies that have this responsibility. We do not want to undo the work done there, but it is not an answer to everything."

## AI SAFETY INSTITUTE SHOULD HAVE A BROADER REMIT

When the House of Commons Science and Technology Committee published, in May 2024, its third and final report from its inquiry into the Governance of Artificial Intelligence<sup>3</sup>, it proposed that AI models and tools should be subject to independent testing. When asked about which bodies could take on this role, Hall referred back to the AI Safety Institute, but said she prefers to talk about auditing.

She explained that the AI Safety Institute was set up by then Prime Minister Rishi Sunak who was very much influenced by big tech arguments that generative AI could present an existential threat.

Hall continued "I did not believe

that there would be any such risk in the near future. These tools do very clever things, but they only analyse information that already exists – there is no intelligence there or cognitive skills. The institute was set up because of a misguided worry about these systems going rogue – the existential threat. An Institute that looks at the safety of these new products and technologies for the general public now is what we need. The AI Safety Institute needs to be much broader in scope."

"The UK could become world-leading in the area of AI safety if we do this well. Auditing comes into this as companies using AI would need to demonstrate that what they use is safe," she said.

## ROLE OF AI FOR HUMANITY

Hall explained that generative AI is a catalyst for new thinking – a new technology that is profoundly clever and will change the world for words and pictures in the same way that the calculator changed things for arithmetic, as we can become much more creative when free from routine tasks. But trust is essential.

"Even with good data quality, Gen AI can get the answers wrong. We cannot rely on it as it can hallucinate. There will be tools that will enable us to be more creative – for example in health, personalising medicine and the creation of new drugs, as well as making hospitals more efficient. But AI will not replace humans in any wholesale way – we need to make AI part of the human team. AI will not make all the decisions; it is just not good enough at the moment to be trusted completely. We also still need to check the data. The data on the Internet is awfully biased and we cannot change that overnight."

## DATA PROTECTION ISSUES IN AI

Many aspects of AI and data protection overlap – and the new Data Bill includes proposals that would affect

AI-generated automated decision-making. How can we find solutions that are fit for the digital world and respect individual rights?

Asked about a situation in recruitment where names and nationalities could be removed to allow for a more bias-free recruitment process, Hall said that AI can in some cases be clever enough to put the name back in, based on other information available.

The Internet is no longer a trusted source of information in the way it was at the very beginning, Hall said. But apps can be developed that analyse just a particular pool of data. For example, in the HR context, to avoid bias, the system would only filter the data it was given.

“In that environment, if you remove the identifying data, you would not allow AI to access the Internet and make biased decisions.”

“You can tell AI not to provide an answer if it does not know the answer.”

Part of the problem lies in awareness or the lack of it. The nation as a whole needs to learn how to distinguish misinformation etc. Privacy and AI education is needed at schools – Hall would start by focussing on the 12+ age group.

“We do not have the resources to do everything at once. We would have to train the teachers first before starting to educate other than in the broadest sense at primary school levels.”

“Also, all university students should have access to an AI course, but this is a struggle currently, even at my own university because of the pressure on resources.”

Hall said she is disappointed that the current government has taken its eye off skills development. According to her, this is not currently on the radar of the Department of Education, even though AI skills are needed at all levels.

Generally speaking, don’t rush to use AI everywhere before we understand it better, Hall advised.

A private member’s Bill, currently in the House of Lords, proposes to make it mandatory to educate workers about AI in the public sector, something that Hall wholeheartedly supports. The Public Authority Algorithmic and Automated Decision-Making Systems Bill<sup>4</sup>, introduced by Lord Clement-Jones (Liberal Democrat) tries to ensure that algorithmic and automated decision-making systems are deployed in a manner that accounts for and mitigates risks to individuals, public authorities, groups and society as a whole, and lead to decisions that are understandable. The Bill also introduces an independent dispute resolution service.

#### INTERNATIONAL ASPECTS OF AI

The UK was one of the first countries to sign the Council of Europe’s AI Convention<sup>5</sup> in September 2024. Hall did not think this was a very significant

development as it was somewhat overshadowed by work at the United Nations, and the UN’s advisory body’s recent report on AI calling for a globally inclusive and distributed architecture for AI governance based on international cooperation<sup>6</sup>.

“The CoE Convention was overtaken by events. The UN recommendations may of course not be successfully implemented – the UN is considering the Report now. We make the point that there are a few different global players that have an interest in AI, such as the OECD, G7, G20, EU, Council of Europe – but the number of countries involved is small. Everyone needs to be involved as suggested by the title of our report, *Governing AI for Humanity*. A global regulation is needed.”

#### REFERENCES

- 1 [bills.parliament.uk/bills/3825](https://bills.parliament.uk/bills/3825)
- 2 [www.gov.uk/government/news/game-changing-tech-to-reach-the-public-faster-as-dedicated-new-unit-launched-to-curb-red-tape](https://www.gov.uk/government/news/game-changing-tech-to-reach-the-public-faster-as-dedicated-new-unit-launched-to-curb-red-tape)
- 3 Dame Wendy Hall gave evidence in this session, see [publications.parliament.uk/pa/cm5804/cmselect/cmsctech/38/report.html#heading-10](https://publications.parliament.uk/pa/cm5804/cmselect/cmsctech/38/report.html#heading-10)
- 4 [bills.parliament.uk/bills/3760](https://bills.parliament.uk/bills/3760)
- 5 [www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence](https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence)
- 6 [www.un.org/en/ai-advisory-body](https://www.un.org/en/ai-advisory-body)

## ICO consults on its approach to fines in the public sector

The ICO has launched a consultation on the scope of its approach to fining the public sector. In 2022, the ICO announced that the Commissioner would use his discretion to reduce the impact of fines in the public sector. While the ICO now says that this approach continues on the whole, it declares that “we intend to adjust it in line with the learnings from the trial period and the responses and input received from this consultation.”

The ICO proposes that it will only issue a fine to a public authority “in the

most egregious cases, that is where the infringements are especially serious”. The ICO suggests that egregious cases might include situations where the case concerns:

- Actual or potential harm to people – this could be physical or bodily harm, psychological harm, economic or financial harm, discrimination, reputational harm or loss of human dignity.
- Intentional or negligent character of the infringement, where there is evidence of intent on the part of the

controller, or a high degree of negligence.

- Relevant previous infringements, or recent infringements, by the controller or processor.

The ICO seeks stakeholders’ views on the definition of those organisations that will fall within scope of the public sector approach, and the circumstances of an infringement that is likely to be regarded as egregious.

- *The consultation closes 31 January 2025. See [www.smartsurvey.co.uk/s/PSA2025/](https://www.smartsurvey.co.uk/s/PSA2025/)*

# Privacy by Design through certification and standards

Ralph O'Brien of REINBO Consulting discusses developments with certifications that publicly recognise good practice and help companies to demonstrate Privacy by Design.

I've always been a huge fan of certification – the ability to be independently assessed and approved that your product, services or organisation meet a certain level of conformance, or meet a certain standard.

Certification can be a wonderful validation that a company is doing something right. But the certification market can be confusing and hard to interpret at times. Different certifications apply to different aspects of a company's operation. The menagerie of players (certification bodies, assurance assessors, scheme owners) can be mind-numbing.

I am involved in this work through the Institute of Operational Privacy by Design (IOPD), which is a not-for-profit set up in the US<sup>1</sup>, but operating globally to create standards and certifications. The IOPD is a membership-based professional organisation primarily run by a Board of Directors consisting of eight volunteers. It tries to untangle the mess created by various different actors and find its own role in this vast and complex ecosystem.

There are many privacy certifications currently on the market, including:

- The European Data Protection Seal
- MSEC ISO 31700-1:2023 – Privacy by Design Framework
- LOCS:23 Standard
- CARU Safe Harbor Program
- TRUSTe Enterprise Privacy Certification
- ISO/IEC 27701:2019
- as well the IOPD Design Process Standard and the forthcoming

Privacy by Design and Default Trustmark.

The IOPD has now introduced the *Design Assurance Standard*<sup>2</sup> for public comment. It seeks to demonstrate achievable objectives with regard to the design, development, and deployment of products, services and business processes. Hopefully DPOs can use it in discussions of how to improve privacy in their organisations which can in turn measure designs for their privacy-friendliness. Regulators will also benefit as they can use the Standard as a benchmark to assess statements of “Privacy by Design and Default”.

## THE WORK OF THE IOPD

The IOPD adopted the *Design Process Standard*<sup>3</sup> (Process Standard) in January 2023 with the *Design Assurance Standard* (Assurance Standard) following almost two years later. While the earlier Process Standard details the components necessary in a design process to incorporate privacy considerations and reduce privacy risks, the new IOPD Assurance Standard uses a specific assurance case to confirm an organisation's claim that a specific product, service, or business process has been designed, developed, or deployed with Data Protection in mind first.

In other words, the Assurance Standard doesn't apply to an organisation but to a specific object of evaluation. The intent of this certifiable standard is for organisations to demonstrate that they have achieved

reasonable assurance around “Privacy by Design and Default” claims.

This is only a draft. Based on the feedback, the Standards Committee will finalise the draft and release the final Design Assurance Standard V. 1.0 in 2025. The draft was open for comment until 1 November 2024, and the committee is now busy reviewing comments and making any appropriate changes as a result.

## THE CERTIFICATION ECOSYSTEM

I've learned a lot about certification in two years as I planned, researched and began to identify the best course of action to create these standards. While different certifications across industries apply different terms, I've tried to consolidate a common description of the “certification” ecosystem. At the core are organisations that want to get something (often referred to as the target or object) certified and an entity or body that provides the certification. Beyond that are various organisations meant to ensure the certification offered is not done in a perfunctory manner, in order to maintain the integrity of the certification.

Here are some of the most common roles in the certification ecosystem:

- **Organisation/Applicant** – The Organisation applies for certification for a product, service, system, business process, or other target of certification.
- **Certification Body** – The Certification Body reviews applications for certification against the scheme and grants or denies certification. The

## ICO CERTIFICATION SCHEMES

The ICO has so far adopted five certification schemes. The most recent one, The Legal Services Operational Privacy Certification Scheme (LOCS), was adopted in February 2024. LOCS is designed to assist legal service providers demonstrate compliance with UK data protection law

when processing client's personal data. It will provide enhanced trust and confidence that personal data and data subject rights are protected.

The ICO has previously approved certification schemes for secure re-use and disposal of IT assets, age assurance and

children's online privacy, and a scheme aimed at training and qualification service providers.

• See [ico.org.uk/for-organisations/advice-and-services/certification-schemes/certification-schemes-register/i-o/](https://ico.org.uk/for-organisations/advice-and-services/certification-schemes/certification-schemes-register/i-o/) and *PL&B UK Report, March 2024, p.9.*

role of the certification body is limited to assessing the four corners of the application, not to assess the conformance of the organisation to the standard. In other words, if the standard criteria says “The organisation must have at least five employees” and the application for certification says the applicant has ten employees, the certificate is issued. Many certification bodies play the role of assessor (see below). An assessor would actually check the payroll of the applicant and assess that the application is accurate and the applicant actually has more than five employees. In that case, the entity is playing two roles: that of certification body, issuing the certification, and that of assessor, assessing the conformance of the applicant to the standard.

- **Assurance Assessor** – The Assessor assesses the target (sometimes called the object of evaluation) of certification for conformance to the scheme criteria. A target could be a business process, a product, a service, a business unit or whatever the scheme purports to evaluate. When an Assessor is not the issuing Certification Body, typically they are trained, approved or otherwise sanctioned by the Certification Body, who is relying on the accuracy of their assessment.
- **Accreditation Agency (Assessor)** – An Accreditation Agency accredits assessors to ensure their assessment process is thorough, accurate, and meets quality standards for assessors. Sometimes this is the Certification Body, but in more mature certification mechanisms this may be a distinct entity. Accreditation need not be to the particular standard the applicant is applying for, but may be to more general qualities (such as security assessments or financial

assessments). Many assessors may themselves be certified as compliant with ISO 9001 for quality management in their assessment process, thus the issuer of that certification to the assessor would be in the role of Accreditation Agency.

- **Accreditation Agency (Certification Body)** – An Accreditation Agency accredits certification bodies to ensure their accreditation process is thorough, accurate, and meets quality standards for certification bodies. Similar to the Accreditation Agency above, the accreditation of the certification body is likely not specific to the standard(s) they are certifying.
- **Scheme Owner** – The Scheme Owner owns and manages the standards or criteria by which a target or object is to be evaluated. They provide the standard to the certification body.
- **Scheme Approver** – Sometimes standards need to be approved by a higher authority, such as a government agency.

Even fairly mature certifications may not have independent actors in each role. As a nascent certification, the planned role of the IOPD is to be the Scheme Owner (we’re the entity developing and managing the standard) as well as the Certification Body (we will issue certifications). Eventually, as we mature, we would like to be accredited, possibly by ANAB<sup>4</sup>, which is the American National Standards Institute Accreditation Board for certification bodies. Our plan is to allow both self-assessment and attestation by applicants and third-party assessments by assurance assessors. This is similar to the Cloud Security Alliance (CSA) model which has STAR Level 1<sup>5</sup> for self-attestations and STAR Level

2<sup>6</sup> of third party audits for their various certifications.

**GOING FORWARD: APPLYING FOR EDPB APPROVAL**

As a long-term goal, we’d like to get the standards approved by the European Data Protection Board (EDPB) as a recognised certification for Article 25 Data Protection by Design and Default under the GDPR. As you can see, we have discussed the standard using the US terminology, and our next step is to rewrite the standard using EU terms, and then introduce this to an EU Supervisory Body to sponsor us in gaining certification approval under GDPR Article 42.

We have a long road ahead and would love your help in getting there. If you’re interested in getting involved, please consider joining<sup>7</sup> as an Ambassador, encouraging your organisation to sponsor<sup>8</sup>, or volunteer<sup>9</sup> in other ways.

To start with, the IOPD Standard is a conformance standard, which means that an organisation will be able to certify that it follows the standard for a given product or service. For each component, the standard provides evidence and evaluation criteria. Currently, the IOPD is developing the certification process and looking for companies that wish to apply for early consideration.

**AUTHOR**

Ralph O’Brien is Principal of REINBO Consulting.  
Email: robrien@reinboconsulting.com

**REFERENCES**

1	<a href="https://instituteofprivacydesign.org/content/uploads/2023/01/Design-Process-Standard-v1.0-Final.pdf">instituteofprivacydesign.org/content/uploads/2023/01/Design-Process-Standard-v1.0-Final.pdf</a>	Two
2	<a href="https://instituteofprivacydesign.org/wp-content/uploads/2024/09/Design-Assurance-Standard-PUBLIC-DRAFT-10.1.24.pdf">instituteofprivacydesign.org/wp-content/uploads/2024/09/Design-Assurance-Standard-PUBLIC-DRAFT-10.1.24.pdf</a>	7
3	<a href="https://instituteofprivacydesign.org/wp-content/uploads/2023/01/Design-Process-Standard-v1.0-Final.pdf">instituteofprivacydesign.org/wp-content/uploads/2023/01/Design-Process-Standard-v1.0-Final.pdf</a>	8
	4 <a href="https://anab.ansi.org/">anab.ansi.org/</a>	9
	5 <a href="https://cloudsecurityalliance.org/star#tab_level">cloudsecurityalliance.org/star#tab_level</a>	
	6 <a href="https://cloudsecurityalliance.org/star#tab_level">cloudsecurityalliance.org/star#tab_level</a>	
		7 <a href="https://instituteofprivacydesign.org/supporters/individual-ambassadors/">instituteofprivacydesign.org/supporters/individual-ambassadors/</a>
		8 <a href="https://instituteofprivacydesign.org/supporters/corporate-members/">instituteofprivacydesign.org/supporters/corporate-members/</a>
		9 <a href="https://instituteofprivacydesign.org/contact-us/">instituteofprivacydesign.org/contact-us/</a>

# Risk, revenue, and relationships: A case study

Sometimes the best privacy outcomes can be achieved by framing the issue in business terms and involving people from different departments. **By Lauren Reid of The Privacy Pro.**

I speak, write and teach about privacy metrics, privacy risk management, and the role of the privacy architect. These subjects make perfect sense (in my unbiased opinion), but what do they look like in real life? Let me share a real example from my consulting practice; a few details have been changed to protect the confidentiality of my clients and possibly entertain you.

The role of a privacy pro often involves navigating tension — between legal compliance, business goals, and user experience.

A few years ago, I found myself in the middle of such a situation at ACME Co., a Canadian wholesaler that sells anvils, catapults, and rocket-powered roller skates to niche retailers of tactical equipment for wildlife enthusiasts.<sup>1</sup> Demand is specialized, and competition is fierce. I was there to support the Chief Privacy Officer as the company expanded to the US market. What unfolded was a journey from conflict to collaboration, and it serves as a blueprint for managing risk by aligning business priorities.

## THE PROBLEM: COMPLIANCE VS REVENUE

ACME’s success hinged on great search engine optimisation and content marketing, thanks to the leadership of Elmer, the VP of Marketing. The product team published white papers on physics and often held free webinars on strategies for deceptive design. Elmer’s team had recently implemented a registration wall on the website, requiring users to submit their contact information to access gated resources. For every 1,000 people who submitted their personal information, ACME converted 3% to sales, to the tune of \$10.8 million in revenue.

Elmer’s team had completed a Privacy Impact Assessment (PIA) when they implemented the registration wall; since it was a lower priority, the web form had been in place for a few

months by the time Sylvester from the compliance team reviewed the PIA. Sylvester noted the web form was not compliant with email marketing laws because it didn’t include a separate unchecked opt-in box. He provided Elmer with specific instructions for how to configure the form and the language to use; it was an easy fix as the functionality was built into the web form’s Software Development Kit (SDK). It did not go well.

Elmer was frustrated—he felt that a checkbox was not only visually unpleasant but would also reduce leads and negatively impact revenue. Sylvester, however, had a mandate to ensure compliance. Both were acting rationally and in ACME’s best interests, but the situation felt gridlocked.

## THE APPROACH: PRIVACY RISK MANAGEMENT

The privacy profession generally agrees that a “risk-based approach” is required. I’m a proponent of using established Enterprise Risk Management discipline. For brevity, I have skipped over a discussion of risk appetite and risk tolerance. The steps in this case study are:

1. Identify and assess risks (Inherent Risk = Likelihood x Impact)
2. Agree on a risk treatment plan (Avoidance, Mitigation, Transfer, Acceptance)

3. Implement controls to reduce inherent risk (Inherent Risk - Effectiveness of Mitigating Controls = Residual Risk)
4. Monitor and manage risk

The privacy risk matrix below is a simple tool I use for calculating risk.

The case study illustrates the approach I take with my clients — your mileage may vary. After two decades, I have gleaned some insights and developed some opinions.

I have observed that privacy risk assessments often fail to consider *non-privacy risks*. A Legitimate Interest Assessment balances the rights of the individual with the interests of the organisation; that concept should be reflected in the risk assessment as well, even if Legitimate Interest is not the legal basis, even in a jurisdiction that doesn’t recognize it. For this reason, I consider business impact alongside privacy harms and compliance.

Privacy risk assessments often fail to consider the *risks of inaction* alongside the risks of action. When evaluating a decision—like using certain data or launching a new product—it’s easy to focus solely on the potential harms of proceeding, such as data breaches, regulatory fines, or reputational damage. However, not taking action carries its own risks: people may lose out on

**A PRIVACY RISK MATRIX**

		Rare	Occasional	Likely
<b>IMPACT</b>	Significant	Medium	High	Critical
	Moderate	Low	Medium	High
	Minimal	Negligible	Low	Medium
		<b>LIKELIHOOD</b>		

the benefits that data use could provide, or the business may forfeit revenue, competitive advantage, or innovation opportunities. Inaction is not a neutral state; it is a choice with consequences. A robust risk assessment requires weighing both sides — understanding the risks of doing something and the risks of not doing it — to make an informed and balanced decision.

I speak to a lot of people who use a “risk-based approach” to set priorities. They focus on the things that can get them in trouble or invest more in protecting sensitive data. I rarely see programs that explicitly acknowledge the risk that people are harmed sometimes. There are compelling business reasons for that reluctance, but I personally believe that until we are able to be honest about risk, we don’t deserve trust. The privacy world has borrowed concepts from the financial services world but stopped short of providing the transparency that empowers individuals to make informed choices. I digress.

**STEP 1: IDENTIFY AND ASSESS RISKS**

We started with two options at either end of the spectrum, knowing we wanted to land somewhere in the middle. Option A is to keep the web form as-is (no opt-in) and accept the risk of harm to individuals, non-compliance with privacy laws, and loss of revenue. Option B would be to modify the web form to include separate, granular consent for outreach. Force opted-out status for everyone who signed up in the last few months using the non-compliant form.

We looked at three potential consequences of changing, or not changing, the web form:

1. Harm to individuals.
2. Enforcement for non-compliance with privacy laws.
3. Loss of revenue.

**HARM TO INDIVIDUALS**

Privacy professionals usually start here, and for a good reason: protecting individuals is why we do this work.

**Option A: Keep the form as-is (no opt-in):**

*Likelihood of harm: Rare*

The relevant privacy harms<sup>2</sup> here stem from personal information being

used for an unexpected purpose (failure to inform) or in a way they didn’t want (disturbance).

Elmer made the point that gated content is a widespread practice. Users generally understand that exchanging their information for a valuable document means the company will contact them, so a reasonable person would not be surprised by the use of their data for this purpose.

*Impact of harm: Minimal*

The website targets employees of organisations that sell tactical equipment to wildlife enthusiasts. These users are not vulnerable, and the only personal information collected via the form is business email and phone number — nothing sensitive.

*Based on the Privacy Risk Matrix, with Option A, the inherent risk of harm to individuals is Negligible.*

**Option B: Modify the form (explicit opt-in):** Option B would eliminate the risk of harm resulting from the use of data for email marketing purposes without explicit consent.

Modifying the form would ensure that even people who are not familiar with common practices around registration walls and gated content are well-informed and given a choice.

Forcing the opt-out status for users who completed the form prior to the update would ensure that no one is contacted who did not explicitly ask to be contacted.

*With Option B, there is no inherent risk of harm to individuals.*

**ENFORCEMENT FOR NON-COMPLIANCE WITH PRIVACY LAWS**

As a Compliance Analyst, Sylvester’s primary concern was complying with privacy laws, which require explicit opt-in consent (via an unchecked box) for email marketing. Note to reader: for the purpose of this case study, the specific law doesn’t matter — stay with me.

**Option A: Keep the form as-is (no opt-in):**

*Likelihood of enforcement: Rare*

When we evaluate the risk of non-compliance, we are mainly concerned with the risk of consequences related to non-compliance, including regulatory investigations, orders, fines, or litigation. These are all separate issues, but for this article, I’ll group them and

refer to them as “enforcement” to keep it simple. In the ACME risk assessment, we examined each one and each law separately.

To determine the likelihood of enforcement, we look at regulator behavior, stated priorities, and litigation trends. In the case of ACME, this was non-existent for B2B Email Marketing, so we assessed the likelihood as Rare.

*Impact of enforcement: Moderate*

Regulatory fines are usually the least concerning impact of enforcement. However, the cost of an investigation, even if unfounded, can be astronomical. Consider the legal fees and the time it takes people away from their jobs.

Some types of enforcement can kill a business, such as an order to delete data or an algorithm. An outstanding lawsuit, even if frivolous, may block a transaction or deter investors.

In the case of ACME, we calculated the Impact to be Moderate based on the privacy team’s limited bandwidth for handling an investigation.

*Based on the Privacy Risk Matrix, with Option A, the inherent risk of enforcement is Low.*

**Option B: Modify the form (explicit opt-in):** Option B would eliminate the risk of non-compliance with email marketing laws because ACME could demonstrate the consent was meaningful:

- **Specific and informed:** Provide clear information about how the personal information would be used for the secondary purpose of email marketing.
- **Timely:** Obtain consent prior to collecting the personal information.
- **Freely Given:** Allow users to download the content without opting in to email marketing.
- **Revokable:** Include an unsubscribe link in all emails.
- **Unambiguous:** Configure the box to be unchecked by default.
- **Demonstrable:** Configure the web form SDK to maintain records of consent.

*With Option B, there is no inherent risk of enforcement.*

**LOSS OF REVENUE**

ACME converted 10% of its website visitors into potential leads by asking

them to provide their contact details in exchange for access to valuable content. Of those leads, 20% were qualified as candidates for sales outreach, and about half of those responded with enough interest to move further in the process. In the end, 35% of these opportunities turned into deals, each worth \$30,000 on average. So, 10,000 website visitors generate roughly \$900,000 in revenue each month, or \$10.8 million per year.

**Option A: Keep the form as-is (no opt-in):**

*Likelihood of lost revenue: Rare*

The web form collects personal information, but it does not ask separately if the Sales team can use the data for outreach. This could lead to people feeling annoyed with the contact and blocking the sender or reporting it as spam.

If a large number of people report your emails, your email address or domain may be blocked. This means your emails are likely to end up in spam folders or be completely blocked by email providers.

In ACME’s case, people voluntarily provided their personal information and expected marketing messages, so the Likelihood of this happening is Rare.

*Impact of lost revenue: Minimal*

The current metrics are based on the web form as-is, without an opt-in checkbox. Leaving the form as it is would not change it.

*Based on the Privacy Risk Matrix, with Option A, the inherent risk of lost revenue is Negligible.*

**Option B: Modify the form (explicit opt-in):** For this one, we’ll look at Impact first:

*Impact of lost revenue: Significant*

Elmer estimated that adding an opt-in checkbox would result in a 10% drop in leads.

If the number of leads dropped by 10%, the financial impact of modifying the form would be \$1,080,000, everything else being equal.

That is a pretty strong argument against implementing a change designed to reduce already low risks.

*Likelihood of lost revenue: Rare*

But everything else is not equal! Assume that asking for opt-in consent reduces the number of leads by 10%. It also means that 100% of the people on our list have indicated that they want to hear from us.

If that 10% reduction in the number of leads (900 instead of 1,000) leads to a 10% increase in the percentage of qualified leads (22% instead of 20%), the difference in revenue is only 1%.

*Based on the privacy risk matrix, with Option B, the inherent risk of lost revenue is Medium.*

**STEP 2: AGREE ON A RISK TREATMENT PLAN**

The next step was to agree on a Privacy Risk Treatment Plan (PRTTP). ACME’s

privacy risk management protocol only required a PRTTP for medium risks and above. So, for the risk of lost revenue, the options were to:

- **Avoid** the risk: do not implement the change (Option A).
- **Mitigate** the risk: implement controls to reduce the Likelihood and/or Impact of lost revenue.
- **Transfer** the risk: not relevant in this scenario.
- **Accept** the risk: modify the form and force opt-out status for the existing leads (Option B).

Seeing it laid out like this made one thing clear: contacting people who don’t want to be contacted was bad for everyone. In all scenarios, this was the driver for increased risk.

Together, Elmer and Sylvester decided to **mitigate the risk** by implementing controls to reduce the likelihood of lost revenue.

**STEP 3: IMPLEMENT CONTROLS TO REDUCE INHERENT RISK**

In the end, ACME chose a version of Option B. They implemented the opt-in checkbox, but only on a go-forward basis. They did not force opted-out status for people who had previously submitted their information, received communication, and chose not to opt out.

To reduce the likelihood and impact of lost revenue, the marketing team focused on giving users a reason to opt in. They set expectations for how often the individual would be contacted and with what content. The form design was changed to present the opt-in box as an opportunity to receive value rather than a fine-print compliance requirement.

**STEP 4: MONITOR AND MANAGE RISK**

We asked Elmer to report on lead volume after the form change. Given the short time the registration wall was in place prior to the intervention, it was difficult to assess, but he was no longer concerned about lost revenue due to the opt-in box.

Anecdotally, the Sales team gave mixed reviews. One person appreciated receiving more qualified leads, while the other felt frustrated with having fewer leads.

**SUMMARY OF ANALYSIS**

	Consequence	Likelihood	Impact	Risk
<b>Option A</b> Keep the form as-is (no opt-in)	Harm to Individuals	Rare	Minimal	Negligible
	Enforcement	Rare	Moderate	Low
	Loss of Revenue	Rare	Minimal	Negligible
<b>Option B</b> Modify the form (explicit opt-in)	Harm to Individuals	None	None	None
	Enforcement	None	None	None
	Loss of Revenue	Rare	Significant	Medium

THE OUTCOME

I'm sharing this experience of what privacy risk management looks like in practice because I'm proud of the outcome: peace! We met people where they were, found common ground, and carved a path that felt like a win for everyone.

We didn't say 'no,' and we didn't use phrases like 'privacy by design,' 'customer trust is paramount,' or 'privacy is good for business.' All of those things are good and true, but shouting them at people who have their own goals to worry about is not the best way to achieve privacy outcomes.

This is privacy in practice:

empowering teams to make better, risk-informed decisions that respect individuals, comply with laws, and drive business success.

If you give people the information they need to make good business decisions, they will.

AUTHOR

Lauren Reid is the Founder of The Privacy Pro.  
Email: lauren@theprivacypro.com

REFERENCES

- 1 All characters, events, and depictions in this case study are fictional. Any resemblance to real persons, living or dead, or to copyrighted characters or entities is purely coincidental. No infringement of any intellectual property rights is intended or should be inferred.
- 2 Citron, Danielle Keats and Solove, Daniel J., Privacy Harms (February 9, 2021). GWU Legal Studies Research Paper No. 2021-11, GWU Law School Public Law Research Paper No. 2021-11, 102 Boston University Law Review 793 (2022), Available at SSRN: [ssrn.com/abstract=3782222](https://ssrn.com/abstract=3782222) or [dx.doi.org/10.2139/ssrn.3782222](https://dx.doi.org/10.2139/ssrn.3782222)

# Teens ask social media companies to protect their mental health

The UN Convention on the Rights of the Child<sup>1</sup> represents a consensus in principle. But how do its principles apply to children's use of social media in practice? **Stewart Dresner** reports.

“Some 80 per cent of children living in developed Western countries have a digital footprint before they are two years old, (largely due to the actions of their family members)”<sup>2</sup> declared *Paul Breitbarth*, Member of Jersey's Data Protection Authority. He provided this attention-grabbing statistic when introducing the panel of four female teenage students from the Hautlieu School in Jersey.

This session was a high point of the Global Privacy Assembly (GPA), organised at the end of October by Jersey's DPA. Resolutions on children's issues had been adopted at previous GPAs in Morocco in 2016 and Mexico in 2021. But this 46th conference was

the first time that teenagers have had an opportunity to give their views on social media to this specialist international audience.

Similar youth panels provide their opinions to the Information and Privacy Commissioner of Ontario, Canada and elsewhere, and some of the social media companies, such as TikTok, have their own youth panels.

The privacy teams at the major social media companies subsequently told me that they paid careful attention to the views of these articulate and engaging members of the Jersey Youth Panel Assembly. Several social media companies are facing litigation in the US and sanctions in Europe. So this session led to some reflections among

their privacy staff who are more aware than anyone else about the advantages, the mental health dangers and the addictive nature of social media platforms.

IS PRIVACY STILL IMPORTANT?

The answer was yes but it is difficult to achieve. The reason is that teens are enthusiastic to download an app but, like adults, they do not read all the privacy conditions. They download the app to share in what their friends are doing. One said “Privacy is hard to control. I don't know where data is shared.”

Many teens know that they can check their privacy settings, for example, on Instagram. But they are unclear as to how their data is being used, for example, to train AI or for other purposes. “My information is being used for what I may have consented to, but I do not necessarily understand the settings.” Some platforms provide different privacy policies for different age groups and/or set a time to read through the privacy policy so the user cannot scroll through them in seconds. However, there is a difference between reading the policy and understanding the implications.

STATISTICS ON TEENS' USE OF SOCIAL MEDIA

Teens are heavy users of social media. According to a Pew Research Center survey of teens aged 13-17 conducted in the US<sup>3</sup> in September/October 2024, and published on 12 December 2024, 90% of them use YouTube, 63% use TikTok, 61% use Instagram and 55% use Snapchat. The survey report states: “Overall, 73% of teens say they go on YouTube daily, making YouTube the most widely

used and visited platform we asked about. This share includes 15% who describe their use as ‘almost constant.’ Roughly half of teens say they go on Instagram or Snapchat every day, including about 10% who say they're on each of these platforms almost constantly. About 60% visit TikTok daily. This includes 16% who report being on it almost constantly.”

Regarding content, “I don’t understand why I am seeing things shown to me. In no way are they harmless,” was a typical comment.

### PROTECTING PRIVACY – TECHNIQUES

Some of the teens use multiple accounts to separate their public and private personas. They often want to protect their private lives as they develop specific interests, some of which might diverge from their home’s cultural or religious norms. “My family does not have access to my private account,” and “I keep different parts of my life private.”

They sense that everything is linked. “You can’t keep things really private. You may attract ‘followers’ but then get contacted by scammers.”

### MENTAL HEALTH

The US Surgeon-General issued a public statement in May 2023<sup>4</sup> listing both benefits and harms of social media. The teen panel in Jersey reported harms such as addiction, anxiety, being subject to harassment and becoming victim of hate-based communication. The constant receiving of information takes its toll. The teens reported that “It is hard to concentrate on a subject in school after lack of sleep,” with its inevitable impact on academic results.

Members of the teen panel were emphatic: “We need to realise that addiction is not healthy....There is a risk to watching other people’s lives,” for example, being absorbed by their phone at a party.

The teens said that some company videos are patronising in tone with messages, such as “Go outside” and “Get off your phone. Socialise.”

### BANNING PHONES IN SCHOOL?

Breitbarth mentioned that in his home country, the Netherlands, mobile phones are prohibited in schools as a

#### THE UN CONVENTION ON THE RIGHTS OF THE CHILD

##### Article 16 (right to privacy)

Every child has the right to privacy. The law should protect the child’s private, family and home life, including protecting children from unlawful attacks that harm their reputation.

##### Article 17 (access to information from the media)

Every child has the right to reliable information from a variety of sources, and governments should encourage the media to provide information that children can understand. Governments must help protect children from materials that could harm them.

new policy starting in the current school year. One of the panel members responded: “I enjoyed school where phones were banned.” Another said “Banning phones in school has advantages. You can use them at home.”

They gave the following anecdotes:

- Some people walk around with phones and don’t have in-person friends.
- Some people text each other from one side of the playground to the other side rather than talk to them.
- Even if phones are banned in class, many people will be distracted from lessons thinking of the next update of their feeds at the next break time or lunch time.
- Cyber bullying is often not easy to define and therefore does not lead to follow-up disciplinary action because the comments made can be inside jokes which would not be understood by school staff.

### EDUCATION ON SOCIAL MEDIA

Are these behavioural issues discussed at school? The consensus was that not enough time was devoted to this subject. “It is hard to understand social media unless you are in it.” Learning about social media should not be

restricted to IT classes. There should be discussions in class monthly, as messages need reinforcing on how to deal with social media innovations.

### SHOULD THERE BE A BAN ON SOCIAL MEDIA FOR UNDER 16s?

The consensus was no, because in addition to games and social contacts, young people use social media and podcasts to consider their aspirations for the future, develop their interest and understanding of subjects outside their school, and receive information on various aspects of their evolving identity.

Many teens do not access news from conventional news sources. As one said: “I always get news from social media.” This point helps explain why even the well-educated articulate teen panel members spend several hours per day on social media for research as well as fun.

### FINAL ADVICE

The final advice from the school students for the GPA audience was:

1. Social media companies should take into account young people’s experience.
2. Don’t ban social media – every individual is different with different needs.
3. Social media users create a huge digital footprint so make sure young people know how their personal data is shared.
4. Simplify privacy policies.
5. Encourage teen users’ independence by protecting their mental health and reducing privacy harms.

#### REFERENCES

- 1 The convention is signed by 196 countries. See [www.unicef.org.uk/what-we-do/un-convention-child-rights/](http://www.unicef.org.uk/what-we-do/un-convention-child-rights/)
- 2 *Children’s right to privacy in the digital age must be improved.* [www.ohchr.org/en/stories/2021/07/child-rens-right-privacy-digital-age-must-be-improved](http://www.ohchr.org/en/stories/2021/07/child-rens-right-privacy-digital-age-must-be-improved)
- 3 *Teens, Social Media and Technology 2024* by The Pew Research Center. [www.pewresearch.org/internet/2024/12/12/teens-social-media-and-technology-2024/](http://www.pewresearch.org/internet/2024/12/12/teens-social-media-and-technology-2024/)
- 4 *Social Media and Youth Mental Health* by The US Surgeon-General. [www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf](http://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf)

# Join the Privacy Laws & Business community

The *PL&B United Kingdom Report*, published six times a year, covers the Data Protection Act 2018, the Freedom of Information Act 2000, Environmental Information Regulations 2004, 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 at least 10 days in advance. Excludes the Annual Conference. More than one free place with Multiple and Enterprise subscriptions.

[privacylaws.com/reports](https://www.privacylaws.com/reports)

“ The UK and International *PL&B* Reports have been my 'go to' resource for 20 years despite the wide choice of alternate resources now available. ”

Derek Wynne , SVP Privacy & Chief Privacy Officer, Paysafe

## International Report

Privacy Laws & Business also publishes *PL&B International Report*, the world's longest running international privacy laws publication, now in its 37th 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](https://www.privacylaws.com/subscribe)

## Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.