EU AI Act and GDPR: Tracing CJEU case law on automated processing and decision-making

Dan Cooper, **Anna Sophia Oberschelp de Meneses**, **Sam Jungyun Choi**, and **David Brazil** of Covington analyse the recent developments.

Automated processing of personal data, and the related concept of automated decision-making (ADM) have become increasingly significant concepts. ADM, the process of making decisions through automated means without human involvement, is employed across a diverse range of contexts, such as evaluating creditworthiness before approving a loan and conducting automated aptitude tests during recruitment processes. Although ADM was already regulated under the European Community Data Protection Directive,[1] the EU General Data Protection Regulation (GDPR)[2] expanded the scope of protections for individuals subject to ADM. The significance of ADM has gained further prominence in recent years with the increasing use of artificial intelligence (AI) in decision-making and the adoption of the EU's Artificial Intelligence Act (AI Act).[3] There has also been a growing number of court decisions at the national level and clarifications from the Court of Justice of the European Union (CJEU) that have shaped the enforcement and interpretation of data subjects' rights relating to ADM.

This article outlines the EU's privacy and AI regulatory framework governing ADM, with an emphasis on provisions specifically addressing automated processing and ADM. It then explores, at a high level, the CJEU's interpretation of these provisions. Finally, the article examines pending cases referred to the CJEU relating to ADM, and recently adopted or proposed EU legislation that may lead to future CJEU litigation in this context.

Relevant provisions under the GDPR and the AI Act

Under Article 22(1) GDPR, individuals have a right "not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." While ADM can involve profiling, which refers to the evaluation or prediction of personal aspects relating to a natural person, this is not always the case. For example, imposing "speeding fines purely on the basis of evidence from speed cameras" would be ADM that does "not necessarily" constitute profiling. However, there would be an element of profiling if "the driving habits of the individual were monitored over time", and, for example, if the level of fine imposed were "the outcome of an assessment involving other factors, such as whether the speeding is a repeat offence or whether the driver has had other recent traffic violations."[4]

Legal or significant effects on the individual: The GDPR does not categorically ban all automated processing of personal data.

First, the provision applies only to decisions made "solely based" on automated processing, meaning there is no meaningful human involvement in the decision-making process.[5]

Second, Article 22 of the GDPR applies only if the ADM has legal effects or has similarly significant effects on the individual. Legal effects typically arise where the decision impacts a person's legal status, entitlements or contractual rights. Examples of effects that are similarly significant to legal effects might include those relating to automated e-recruiting practices or online credit applications.

Third, ADM is permitted if it meets one of the following conditions:

(1) it is necessary for entering into or performing a contract with the data subject;
(2) it is authorized by Union or Member State law, which includes suitable measures to safeguard the data subject's rights, freedoms, and legitimate interests; or
(3) it is based on the data subject's explicit consent. In cases where automated processing is necessary for a contract or based on explicit consent, the controller must implement measures to protect the data subject's rights, including the right to obtain human intervention, express their viewpoint, and contest the decision.

Informing the data subject: In addition to Article 22 GDPR, the transparency obligations under Articles 13(2)(f) and 14(2)(g) GDPR require controllers to inform data subjects about the existence of any ADM which they carry out about the data subject. The data subject is also entitled to receive information about the presence of ADM and "meaningful information about the logic involved" in the ADM process as part of the controller's response to a data subject access request, pursuant to Article 15(1)(h) GDPR.

Defining the AI System: Aside from the GDPR, the recently adopted AI Act also regulates certain types of ADM. While automated processing does not inherently constitute AI, the two concepts often intersect. Automated processing may range from simple rule-based algorithms to autonomous and adaptive systems that leverage advanced machine learning and pattern recognition techniques. The recently adopted AI Act regulates so-called "AI systems", defined in

Article 3 as a machine-based system that operates with autonomy, exhibits adaptiveness, and is capable of inferring "from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments". If the ADM system meets this definition of "AI system", the AI Act will apply.

Article 86 of the AI Act applies to deployers that take decisions:

(i) on the basis of the output produced by certain types of high-risk AI systems, and
(ii) which produce legal or similar effects towards an individual "in a way that they consider to have an adverse impact on their health, safety or fundamental rights". In such cases, the deployer must provide "clear and meaningful explanations of the role of the AI system in the decision-making procedure and the main elements of the decision taken." The scope of this provision is therefore more limited than Article 15(h) of the GDPR.

CJEU Decisions on ADM Under the GDPR

Two recent CJEU decisions – *Schufa* and *D&B*, discussed below – directly address the concept of ADM as defined and regulated by the GDPR. In both cases, the CJEU examines how Article 22 GDPR applies to processing of personal data for automated credit scoring.

Schufa (C-634/21)[6]: This case concerned Schufa, a German company that assesses the creditworthiness of individuals and supplies such information to its contractual partners. Schufa used a scoring system to predict the probability of future behavior, such as the likelihood of loan repayment, based on certain characteristics of individuals and by relying upon "statistical methods". The case arose when an individual, whose loan was denied on the basis of a negative score calculated by Schufa, requested access to his personal data held by the company, and sought the correction of the allegedly inaccurate information.

The CJEU examined whether generating a creditworthiness score that is subsequently used by third parties for credit decisions, constitutes ADM under Article 22 GDPR. The CJEU analysed the conditions necessary for Article 22 to apply: (i) a "decision" must be made, (ii) the decision must be "based solely on automated processing, including profiling", and (iii) the decision must have "legal effects concerning [the data subject]" or "similarly significantly [affect] him or her."

The CJEU ruled that Schufa's creation of a credit score qualifies as a "decision", as the concept is "broad enough" to include calculating the probability of a person's ability to meet payments. It affirmed that Schufa engaged in "profiling" as defined in Article 4(4) GDPR. Furthermore, it held that even if a third-party makes the final decision, if such an entity draws strongly on the score, such scoring should be considered as solely based on automated processing. Finally, the CJEU concluded that, to the extent that Schufa's customers attribute a decisive role to the creditworthiness score in establishing, implementing, or terminating a contractual relationship with the concerned data subject, this score meets criterion (iii) and thus constitutes ADM under Article 22 of the GDPR.

D&B (C-203/22)[7]: In *D&B*, a mobile network operator denied an individual a mobile phone contract based on insufficient financial creditworthiness. The network operator relied on an automated credit assessment of the individual provided to it by D&B to make this decision. When the individual requested "meaningful information about the logic involved" in the automated decision under Article 15(1)(h) GDPR, D&B provided a response that did not include certain information, on the basis that it constituted a protected trade secret and was therefore not disclosable.

The First Chamber addressed two main issues:

- **Scope of "Meaningful Information" under Article 15(1)(h) GDPR**. The CJEU reiterated that, in cases involving ADM, controllers must provide concise, transparent, intelligible, and easily accessible explanations of "the procedure and principles actually applied" by automated means, to personal data to arrive at a specific result. This explanation should allow the data subject to understand which of his or her personal data has been used in the automated decision-making, but the CJEU did not elaborate on how controllers should describe "the procedure and principles." The CJEU also emphasized data controllers could not satisfy Article 15(1)(h) GDPR through the "mere communication of a complex mathematical formula, such as an algorithm, or by the detailed description of all the steps in automated decision-making" to the data subject, as this would not "constitute a sufficiently concise and intelligible explanation".
- **Balancing Data Subject Rights and trade secrets**. The CJEU noted that the right to the protection of personal data is "not absolute", and must be balanced proportionately against other fundamental rights, a notion that extends to a third party's trade secrets and intellectual property rights. "Wherever possible" controllers should choose the "means of communicating personal data to data subjects that do not infringe the rights or freedoms of others." Where trade secrets are implicated, controllers may need to present the protected information to the competent supervisory authority or court, which should balance the competing interests and determine the extent of the data subject's rights of access.

Other relevant decisions: Two additional CJEU rulings, though not explicitly focused on ADM, are pertinent to automated processing of personal data:

In *Nacionalinis* (C-683/21)[8], the Grand Chamber ruled that joint controllership exists whenever parties influence how and why data is processed, even if they assume different roles or one has a limited role. This has significant implications for automated processing: if both the customer and the vendor of automated processing tools determine processing purposes and means – such as by jointly deciding on data usage, the manner of processing, and objectives –

they may be classified as joint controllers, meaning they both jointly assume the data controller obligations under the GDPR.

In *KNLTB* (C-621/22)[9], the Ninth Chamber confirmed that controllers who rely on Article 6(1)(f) as their lawful basis for processing can do so pursuant to legitimate interests that are not affirmatively or positively established in law, and that commercial interests can constitute legitimate interests provided that those commercial interests are not unlawful. This decision is favorable to automated processing, as it supports relying on legitimate interests as a legal basis to develop automated processing systems, provided that controllers satisfy all other GDPR requirements related to this legal basis, including necessity, proportionality, and balancing against the rights and freedoms of data subjects. Note, however, that legitimate interests is not an exception to the prohibition against ADM with legal or similarly significant effects subject to Article 22 GDPR.

Automated Processing and Fundamental Rights

Aside from decisions relating to the GDPR, the CJEU has also ruled on the use of automated processing in ways that impact fundamental rights, most notably in the areas of law enforcement and counter-terrorism. In these cases, the CJEU balances the security interests of Member States against the fundamental right to privacy. As a general rule, the CJEU has held that government access to data and use of automated tools should be limited to what is strictly necessary.

La Quadrature du Net (C-511/18, C-512/18, C-520/18)[10]: In *La Quadrature du Net*, the Grand Chamber of the CJEU held that French and Belgian statutes obliging telecom and hosting providers to retain and submit all traffic and location data to real-time automated analysis for evidence of potential terrorism for intelligence services exceed the limits of what is strictly necessary, and cannot be considered justified in a democratic society. The Court found such data "may reveal information on a significant number of aspects of the private life of the persons concerned… including sexual orientation, political opinions [and] state of health."

The Grand Chamber also held that general retention could be permissible to safeguard national security against a threat that is "genuine and present or foreseeable." As less intrusive alternatives, it permitted targeted retention based on specific criteria, expedited preservation ("quick freeze") orders, and the real-time collection of data from persons suspected of terrorist activities. These must be subject to prior review by a court or independent body and individuals must be notified afterwards to allow for legal redress.

Ligue des droits humains (C-817/19)[11]: In *Ligue des droits humains*, the Grand Chamber assessed the validity of the EU's Passenger Name Record (PNR) Directive, a measure mandating the mass collection, retention and automated analysis of air passenger data to combat terrorism and serious crime. The Court ruled that this framework establishes a "surveillance regime that is continuous, untargeted and systematic", that amounts to an "undeniably serious" interference with the fundamental rights to privacy and data protection.

To render such automated assessment lawful, the Court ruled data on passengers could be retained for an initial period of six months, not five years, and that extending the system to intra-EU travel could only be permissible when a Member State is confronted with a "genuine and present or foreseeable" terrorist threat, citing *La Quadrature du Net*.

The Grand Chamber also held that the PNR Directive's requirement for "pre-determined criteria" "precludes the use of artificial intelligence technology in self-learning systems ('machine learning')." It reasoned that the opacity of such technology would make it "impossible to understand the reason why a given program arrived at a positive match", thereby undermining the right to an effective remedy.

Potential sources of further CJEU litigation

Referrals to the CJEU: Two pending referrals before the CJEU look set to address concerns regarding the opacity of recommendation algorithms and other complex automated processes.

In *Yettel Bulgaria* (C-806/24)[12], the referring court asks whether, in the context of a consumer dispute over automatically generated mobile phone invoices, Article 86(1) of the AI Act grants consumers the right to demand from service providers a meaningful, intelligible account of the invoicing algorithm. It also asks whether Article 86(1), read in conjunction with other core principles of EU law, permits courts to demand from traders "the black box data, the source code and the algorithm relating to the way in which automated decisions are made under the consumer contract".

The *Rowicz* (C-159/25)[13] referral challenges the Polish system of assigning judges to cases using an automated "random case allocation generator" (SLPS) and asks whether a court can be considered independent and impartial, when neither the source code, nor "the ability to verify the operation of the SLPS algorithm", nor the "ability to ascertain the vulnerability of the random case allocation tool to errors and manipulation" are available. The referral also points to apparent practical failings, suggesting that the SPLS system does not guarantee an "even workload for judges", and may lead to undue delays and discrimination between litigants, in contravention of the right to a fair trial under Article 47 of the Charter. The referral cites Recital 61 of the AI Act, which provides that AI systems intended for the administration of justice should be classified as "high-risk", adding that "it is appropriate to qualify as high-risk AI systems intended to be used by a judicial authority or on its behalf to assist judicial authorities in researching and interpreting facts and the law and in applying the law to a concrete set of facts." It is yet unclear whether the SLPS algorithm would qualify as a high-risk AI system under the AI Act.

Related laws that will give rise to CJEU case law: As the EU's regulatory landscape evolves, it's increasingly likely that AI-related cases before the Court of Justice of the European Union (CJEU) will not be limited to data protection. Two major

new laws—the General Product Safety Regulation and the new Product Liability Directive— may contribute to future CJEU litigation involving AI.

General Product Safety Regulation (GPSR)[14]: The GPSR, applicable since December 13, 2024, requires manufacturers, importers, distributors, and fulfilment service providers to ensure that such products remain safe throughout their lifecycle. This includes ensuring safety after software updates or algorithmic changes, taking into account their "evolving, learning and predictive functionalities, directly implicating AI related features." Online marketplaces are required to implement processes to support product safety, including responding swiftly to orders from authorities to remove unsafe products. The GPSR introduces obligations for risk assessment, ongoing monitoring, and documentation. Legal disputes may arise over the definition of a "safe" AI feature or the adequacy of safety measures—issues likely to be referred to the CJEU as courts interpret these new standards in the context of AI.

Product Liability Directive (PLD)[15]: The revised PLD, finalized in 2024 and applying from October 2026, will further expand the legal framework for AI by explicitly treating software, including AI systems, as "products" for liability purposes.

The revised PLD explicitly requires courts to evaluate the defectiveness of a product by considering the "effect on the product of any ability to continue to learn or acquire new features after it is placed on the market or put into service." This revision clearly aims to address the impact of AI systems on products. Under the revised PLD, service providers and their technology partners could be subject to strict liability for damages resulting from defects in AI-driven services or tools. This liability extends to issues arising from software updates, cybersecurity vulnerabilities, or a lack of transparency in the operation of AI systems.

The revised PLD also introduces presumptions that make it easier for claimants to establish liability when facing complex or opaque AI systems. This means that if an AI-powered platform causes financial loss or other harm, courts may need to determine what constitutes a "defect" or how to allocate liability among multiple parties—issues likely to generate CJEU case law.

Legislative proposals: In addition to existing and recently adopted legislation, the EU is also considering adopting further legislation that will regulate ADM and uses of AI in certain contexts. Two proposals worth mentioning are the Digital Fairness Act and the Directive on Workplace Algorithmic Fairness, both of which are still being considered in the legislative process.

Digital Fairness Act (DFA)[16]: The DFA is expected to tackle "enforcement gaps" in existing consumer legislation, especially as it relates to "the specific harmful practices and challenges that consumers face online". These include, but are not limited to dark patterns, addictive design, and manipulative personalisation in consumer choices and contracts.

The stated objectives of the DFA specifically refer to "problematic personalisation practices", and "addressing unfair practices related to price". Unlike the current EU Consumer Rights Directive, which merely requires a declaration that pricing has been personalized using automated decision-making, the DFA may require the provision of comprehensive information detailing how personalized prices are calculated and whether they advantage or disadvantage consumers.

The DFA may surpass existing GDPR transparency requirements by requiring transparency disclosures at the time offers are made, not only when data is collected or at contract finalization. It seeks to bridge regulatory gaps and fortify consumer rights in digital markets, anticipating its role in shaping new case law in the CJEU regarding ADM and consumer protection in digital contexts.

Directive on Workplace Algorithmic Fairness (WAFD)[17]: The WAFD targets the use of ADM systems in employment settings, emphasizing transparency, fairness, and human oversight in algorithmic decisions affecting workers. It would prohibit digital labour platforms[18] from processing sensitive personal data through ADM, including "emotional or psychological states", "private conversations", "neurosurveillance", "the prediction of the exercise of fundamental rights", or inferences as to special categories of personal data. The Directive would mandate that platforms transparently inform workers, their representatives, and competent authorities about the use, purpose, and functioning of ADM and automated monitoring systems, including detailed disclosures on data categories, decision types, and parameters impacting workers' contracts or payments. This information should be provided clearly, promptly, and upon request, ensuring workers understand how ADM affects their working conditions.

The WAFD would further mandate that employers and procurers of services maintain "effective human oversight at all times" over algorithmic management systems deployed in the workplace, and that human review and intervention should be available for significant automated decisions, such as for hiring, pay changes, or terminations.

Moreover, it would oblige platforms to assess and mitigate safety and health risks linked to ADM, preventing undue pressure or harm to workers. These provisions propose to foster accountability, transparency and workers' fundamental rights, complementing consumer-focused initiatives like the DFA, and extending robust protections against potential harms of automated decision-making in the workplace.

Conclusion

Until recently, the GDPR was the main piece of horizontal EU legislation that regulated ADM. Just as we are gaining more clarity about the applicability of the GDPR to ADM through CJEU cases like Schufa and D&B, other pieces of EU legislation that could apply to ADM are starting to come into force. The AI Act's provisions on high-risk AI systems, including Article 86, will start to apply from 2 August 2026. The GPSR has already started to apply from December 2024 and the PLD will apply from October 2026. New legislative proposals like the DFA

and the WAFD are also being considered.

We anticipate that these new laws will provide a basis for the CJEU to rule on how ADM, and the new technologies that enable it, should be used in the EU, in a way compatible with the EU's commitment to protecting fundamental rights of individuals.

AUTHORS

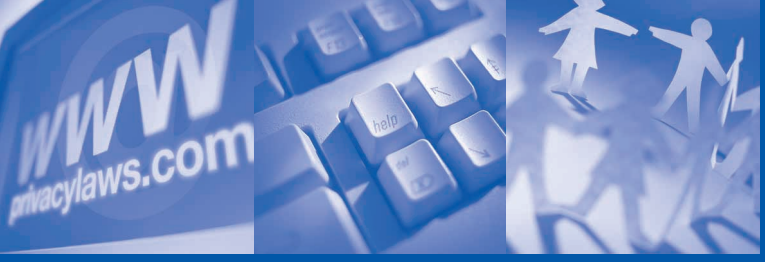
Dan Cooper, Partner; Anna Sophia Oberschelp de Meneses, Special Counsel; Sam Jungyun Choi, Associate; and David Brazil, Associate, at Covington, Belgium.
Emails: dcooper@cov.com
aoberschelpdemeneses@cov.com
jchoi@cov.com,
dbrazil@cov.com

INFORMATION

The authors would like to recognise the contribution to this article by Erin Lynch, Trainee Solicitor at Covington UK.

REFERENCES

1 Data Protection Directive — Directive 95/46/EC (24 October 1995).
2 GDPR — Regulation (EU) 2016/679 (27 April 2016)
3 EU AI Act — Regulation (EU) 2024/1689 (13 June 2024).
4 Article 29 Data Protection Working Party ("A29WP"), 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (WP251rev.01, 6 February 2018)
5 For a discussion of what constitutes "meaningful" human intervention, see *Autoriteit Persoonsgegevens* (Dutch Data Protection Authority). 'Meaningful Human Intervention: A tool for shaping and implementing meaningful human intervention', (July 2025). This paper emphasizes among other things, the competence of the human assessor, and the importance of the assessor's work not becoming "routine, without having an influence on the outcome".
6 Case C-634/21 *SCHUFA Holding (Scoring)* ECLI:EU:C:2023:957 (7 December 2023)
7 Case C-203/22 *Dun & Bradstreet Austria* ECLI:EU:C:2025:117 (27 February 2025).
8 Case C-683/21 *Nacionalinis visuomenės sveikatos centras v Valstybinė duomenų apsaugos inspekcija* ECLI:EU:C:2023:949 (5 December 2023).
9 Case C-621/22 *Koninklijke Nederlandse Lawn Tennisbond v Autoriteit Persoonsgegevens* (KNLTB) ECLI:EU:C:2024:858 (4 October 2024).
10 Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others v Premier ministre and Others* ECLI:EU:C:2020:791 (6 October 2020).
11 Case C-817/19 *Ligue des droits humains v Conseil des ministres* ECLI:EU:C:2022:491 (21 June 2022).
12 Case C-806/24 *Yettel Bulgaria EAD v FB* (request for a preliminary ruling, lodged 25 November 2024), OJ C/2025/1080, 24 February 2025 (ELI).
13 Case C-159/25 *Rowicz* (request for a preliminary ruling, lodged 26 February 2025), OJ C/2025/3261, 24 June 2025 (ELI).
14 General Product Safety Regulation (GPSR) — Regulation (EU) 2023/988 (10 May 2023).
15 Product Liability Directive (PLD) — Directive (EU) 2024/2853 (23 October 2024).
16 European Commission, 'Digital Fairness Act' (Call for evidence for an impact assessment - Ares(2025)5829481).
17 European Parliament, EMPL Committee, Draft report […] on digitalisation, artificial intelligence and algorithmic management in the workplace – shaping the future of work (2025/2080(INL), 26 June 2025) PE774.283v02-00.
18 These include location-based platforms, where the services are provided by individuals in a specific location, and online platforms, where workers provide their services remotely.



ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Defending MAGA-speech: Trump's war on global data privacy

By **Graham Greenleaf**, Honorary Professor, Macquarie Law School, Australia.

Fifty years since the first data privacy laws in the early 1970s[1] the United States and Europe have reached a stalemate in their conflict over the global practices of surveillance capitalism. National governments, particularly in the EU, through much stronger enforcement of data privacy laws, and competition and consumer

Continued on p.3

Australia seeks real-world privacy protections for children

Following the UK and Ireland, Australia is developing a Children's Online Privacy Code. Information Commissioner Carly Kind talked to *PL&B's* **Laura Linkomies** at the GPA in South Korea.

Things are moving fast in Australia. A consultation, including a meaningful opportunity for children to have their say, has now finished[1] and there will be a further statutory consultation period of 60 days on the draft code at the beginning of 2026.

"Engagement by parents and children on the Code has been amazing. We received around 300 responses from them and many more

Continued on p.10

Future *PL&B* Events

Minding the (US-European) Privacy Gap
4 November 2025, Host: Latham & Watkins, London
www.privacylaws.com/USA2025

Meet the Correspondents
3 December 2025, Host: Stephenson Harwood, London
This is a complimentary event for subscribers to *PL&B* Reports.
Come and meet some of our regular correspondents
www.privacylaws.com/correspondents2025

Issue 197 **OCTOBER 2025**

See the publisher's blog at privacylaws.com/blog2025oct

INTERNATIONAL report

ISSUE NO 197 OCTOBER 2025

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

ASIA-PACIFIC EDITOR
Graham Greenleaf
graham@austlii.edu.au

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Graham Greenleaf
Honorary Professor, Macquarie University, Australia

Dan Cooper, Anna Sophia Oberschelp de Meneses, Sam Jungyun Choi, and David Brazil
Covington, Belgium

Farid Bouguettaya
Kalder, France

Hannah Heilbuth
University of Nottingham, UK

Juliette Faivre
PL&B Correspondent, Luxembourg

Wenlong Li
Zhejiang University, China

Yueming Zhang
Ghent University, Belgium

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* International 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 2046-844X

comment

Global DPAs take a close look at AI in Korea

I was pleased to attend the Global Privacy Assembly in Korea in September where Data Protection Authorities and organisations from 95 countries discussed data protection issues with a heavy focus on AI.

While there is no global approach to AI, the Council of Europe's AI Convention tries to create a level playing field where it applies - public authorities and private entities acting on their behalf. The main piece of legislation is the EU's AI Act, adopted in May 2024. Korea itself adopted an AI Act in January 2025, to enter into force in January 2026.

The EU DPAs have been saying for some time that GDPR principles apply to AI and that this framework works well. In the US, the Trump administration is shaping US policy on AI with its AI Action Plan, and revoking the previous administrations' executive orders. Read an analysis by Professor Graham Greenleaf on US developments in the digital field on p.1.

However, there are many state level developments on AI in the US. For example in California, OpenAI is advocating that the state of California aligns its AI rules with international frameworks. It remains to be seen what influence the state-level activity will have at the federal level. Join us at the 4 November conference, in London and online, to find out (p.23).

In this issue, our correspondents analyse why Deepseek is under international DPA scrutiny (p.28) and what stance France's regulator is taking on AI in its recent guidance (p.18). Also, read on p.13 how the EU's privacy and AI regulatory framework governs automated decision-making, and how this is reflected in the CJEU's interpretation of these provisions.

In Korea, I also had an opportunity to interview Australia's Information Commissioner Carly Kind about her office's work on a children's code. Australia is now watched closely by many, also because of its radical policy to ban social media accounts for under 16s (p.1).

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura@privacylaws.com.

Join the Privacy Laws & Business community

The *PL&B International Report*, published six times a year, is the world's longest running international privacy laws publication. It provides comprehensive global news, on 180+ countries alongside legal analysis, management guidance and corporate case studies.

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 180+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and administrative decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance and 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 Version
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 International 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 in advance of the free-place deadline. Excludes the Annual Conference. More than one place with Multiple and Enterprise subscriptions.

privacylaws.com/reports

"I consistently find that both the UK and International publications offer exceptional insights into all facets of data protection, ranging from regulatory requirements to practical lessons learned."

Sharon Terry, Senior Data Protection Manager, Equiniti Group

UK Report

Privacy Laws & Business also publishes *PL&B UK Report* six times a year, covering the Data (Use and Access) Act 2025, the Data Protection Act 2018, the UK GDPR and related regulatory changes, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Electronic Communications Regulations 2003.

Stay informed of legislative developments, learn from others' experience through case studies and analysis, and incorporate compliance solutions into your business.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory, two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

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