



# DATA PROTECTION LEADER

Volume 5, Issue 4  
July 2023  
[dataguidance.com](https://dataguidance.com)

Ideas shaping privacy, published by OneTrust DataGuidance™

## FOUR TRUTHS ABOUT THE DATA PRIVACY FRAMEWORK

---

### EU AI ACT

Exploring  
implementation  
and best practices  
for companies

---

### TEXAS

Analyzing the  
TDPSA and the  
SCOPE Act, as well  
as how to comply

---

### WHISTLEBLOWING

Discussing the new  
legislation in Germany  
and what employer's  
need to do

# CONTRIBUTORS TO THIS ISSUE



## **Eduardo Ustaran, Hogan Lovells**

Eduardo Ustaran is Global co-head of the Hogan Lovells Privacy and Cybersecurity practice and is widely recognised as one of the world's leading privacy and data protection lawyers and thought leaders. With over two decades of experience, Eduardo advises multinationals and governments around the world on the adoption of privacy and cybersecurity strategies and policies. Based in London, Eduardo leads a highly dedicated team advising on all aspects of data protection law – from strategic issues related to the latest technological developments such as artificial intelligence and connected devices to the implementation of global privacy compliance programs and mechanisms to legitimise international data flows.



## **Charles Kerrigan, CMS London**

Charles Kerrigan is a partner in the Finance Team and part of the specialist Crypto and Digital Assets Team at CMS London specialising in emerging technologies including crypto, digital assets, decentralised finance and AI. He works on corporate finance and venture capital transactions in crypto, tokenisation, NFTs, Web3 and DeFi. Charles is part of teams working on investing and setting standards for emtech in the UK, Europe and the US. He works on consulting projects on blockchain and AI for public bodies, policy makers, standards institutions, and corporations. The Blockchain Industry Landscape Overview 2018 names Charles as "one of the UK's leading influencers on blockchain". He is the UK's "recommended lawyer" for blockchain and digital technology in the UK Parliament Hub.



## **Sean Musch, AI & Partners**

As a seasoned tech accountant, Sean leads assurance engagements and reviews. He is an outward facing auditor, owning relationships with clients and other key stakeholders. He specialises in conducting engagements in the tech audit sector and his clientele value his critical thinking and forensic-level analysis.



## **Michael Charles Borrelli, AI & Partners**

Michael Charles Borrelli is a highly experienced financial services professional with over 10 years of experience. He has held executive positions in compliance, regulation, and management consulting for institutional financial services firms. He currently advises AI companies. He also holds an L.L.M. in Financial Regulation and Compliance.



## **Bart Huffman, Holland & Knight LLP**

Bart Huffman is a data strategy, security and privacy attorney. He has a systems engineering and IP background, as well as deep experience in privacy and cyber security matters and sophisticated technology transactions. He leads engagements involving data, information systems and/or operational technology in connection with large-scale SaaS and other cloud-platform implementations, ransomware and data breach response, technology vendor contracting and oversight, domestic and international privacy and cybersecurity compliance projects and programs, business intelligence and data analysis, AI, data enrichment and data analytics, software and information systems development and licensing, legal and contractual cybersecurity risks, and governance advice.



## **Haylie Treas, Holland & Knight LLP**

Haylie Treas is an attorney in Holland & Knight's Houston office and a member of the firm's Data Strategy, Security & Privacy Team. With a background in civil litigation and experience counseling clients in privacy and data security matters, Ms. Treas is able to bring a broad perspective in advising clients in a wide variety of matters, including data breach incident response, regulatory compliance, technology transactions, privacy and security policies and procedures, mergers and acquisitions (M&A) due diligence, and technology and data support. Ms. Treas works alongside companies of all sizes on privacy and security matters spanning the areas of energy, construction, software development, healthcare and cybersecurity. Ms. Treas is also a Certified Information Privacy Professional – U.S. (CIPP/US).



## **Akinkunmi Akinwunmi, Paragon Advisors**

Akinkunmi Akinwunmi is the Lead Partner of Paragon Advisors, a law firm based in Lagos, Nigeria. He is in charge of the law firm's Technology, Media, Telecommunications (TMT) and Business Advisory practice. Akinkunmi is the author of the book, The Nigerian Internet Law. He has advised on setting up of venture capital and InsurTech firms, operations of FinTech and e-commerce companies, start-up financing, intellectual property advisory and portfolio management, and licensing of entities for technology or telecommunications services.



## **Tobias Neufeld, ARQIS**

Tobias Neufeld, LL.M. (CIPPE/E, CIPM, DPO) is a German qualified lawyer, data law specialist, solicitor (England & Wales) and partner in the Düsseldorf office of ARQIS. Previously, Tobias Neufeld was a partner at the international law firm Allen & Overy LLP, where he headed the German data protection practice and was the firm's global head of employment and benefits. Prior to that, he worked as a partner and associate for leading international law firms in London, Frankfurt, Munich and Düsseldorf. Tobias Neufeld advises national and international companies in all areas of data law, privacy, employment and related compliance. He also is a co-founder of byond, a consultancy on digital ethics/corporate digital responsibility and sustainability.

### **Image production credits**

Cover / page 4 image: tiero / Essentials collection / istockphoto.com  
Page 6-7 image: BlackJack3D / Signature collection / istockphoto.com  
Page 10-11 image: thomas-bethge / Essentials collection / istockphoto.com  
Page 16-17 image: Wirestock / Essentials collection / istockphoto.com  
Page 18-19 image: markchentx / Signature collection / istockphoto.com  
Page 22 image: Ramberg / Signature collection / istockphoto.com  
Page 24-25 image: gonin / Essentials collection / istockphoto.com  
Page 26 image: tigrisiara / Essentials collection / istockphoto.com

Data Protection Leader is published bi-monthly by OneTrust Technology Limited, Dixon House, 1 Lloyd's Avenue, London EC3N 3DS

**Website** [www.dataguidance.com](http://www.dataguidance.com)

**Email** [DPL@onetrust.com](mailto:DPL@onetrust.com)

© OneTrust Technology Limited. All Rights Reserved. Publication in whole or in part in any medium, electronic or otherwise, without written permission is strictly prohibited. ISSN 2398-9955

**OneTrust DataGuidance™**  
REGULATORY RESEARCH SOFTWARE

**Editor Eduardo Ustaran**  
[eduardo.ustaran@hoganlovells.com](mailto:eduardo.ustaran@hoganlovells.com)

**Managing Editor Alexis Kateifides**  
[akateifides@onetrust.com](mailto:akateifides@onetrust.com)

**Editorial Lead Victoria Prescott**  
[vprescott@onetrust.com](mailto:vprescott@onetrust.com)



# CONTENTS

- 4 Editorial: Four truths about the Data Privacy Framework**  
By Eduardo Ustaran, Partner at Hogan Lovells
- 6 EU: Prioritizing privacy under the AI Act**  
By Sean Musch and Michael Borrelli, from AI & Partners, and Charles Kerrigan, from CMS London
- 10 Germany: Getting to know the new whistleblowing legislation**  
By Tobias Neufeld and Sebastian Gutzeit from ARQIS
- 14 Infographic: GDPR Fine Enforcement: Q2 2023 Report**  
By the OneTrust DataGuidance Content Team
- 16 Meet a DPO: Fabrizio Venturelli**  
Global DPO at Workday
- 18 State Profile: Texas**  
By Bart Huffman and Haylie Treas, from Holland & Knight LLP
- 22 Five years of GDPR: What is the best way to approach new digital challenges**  
By the Robb Hiscock, OneTrust Editorial Team
- 24 Nigeria: Exploring AI recommender systems through the NDPA**  
By Akinkunmi Akinwunmi, from Paragon Advisors
- 26 5 minutes with: Goli Mahdavi**  
Attorney at Bryan Cave Leighton Paisner LLP

## EDITORIAL

「*The only remaining question about the DPF that nobody can answer with absolute certainty is whether it will survive any eventual scrutiny by the Court of Justice of the European Union*」



# Editorial: Four truths about the Data Privacy Framework



By **Eduardo Ustaran** Partner  
eduardo.ustaran@  
hoganlovells.com  
Hogan Lovells, London

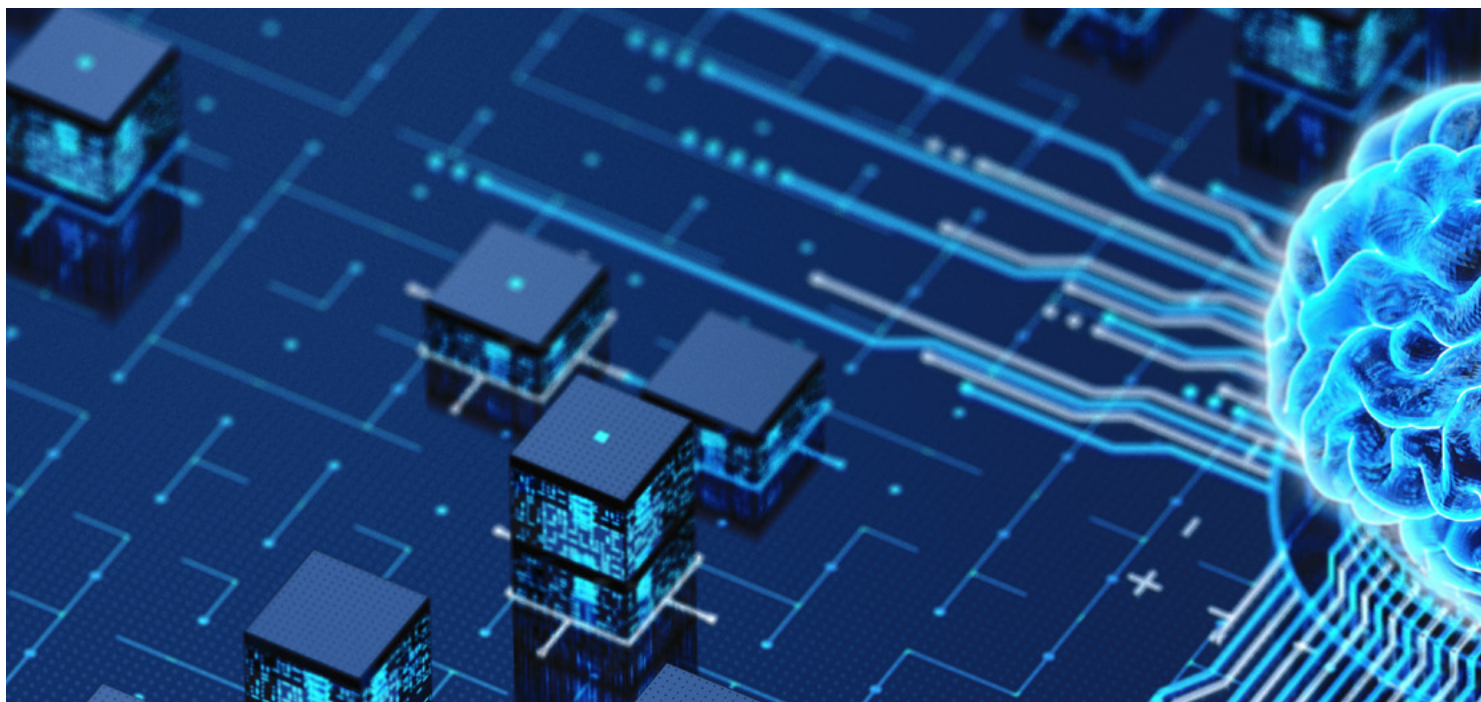
Here we are again. Another Summer, another hugely significant development for international data transfers. In 2020, it was the landmark *Schrems II* decision. In 2021, it was the adoption of the new Standard Contractual Clauses (SCC) and the Summer of 2022 brought with it a sweeping heatwave of extreme regulatory decisions signalling the incurable unlawfulness of every transfer of data to the US involving an electronic communications service provider. This year, the development follows the relentless - and hopefully productive - work of the European Commission and the US Government to finally get it right and agree on a framework that is able to pass the elusive 'adequacy test.' The outcome has been the Commission's adequacy decision on the EU-US Data Privacy Framework (DPF). Given the unbearable pressure on this topic, as highlighted by the aggressive enforcement activity seen this year so far, to say that this is a welcome development is an understatement, but what are the essential truths about it?

**It's all about state surveillance:** What should be obvious by now is that the restrictions on international data transfers, which were originally designed to avoid European data protection becoming redundant in the face of globalisation, have become all about restricting foreign states' surveillance involving European data. This shift on emphasis from data protection governance to government access to data was triggered 10 years ago by Edward Snowden's disclosures and as a result, the attention has exclusively focused on the powers and practices of US government agencies. Therefore, by far the most significant aspect of the DPF from a European perspective is simply the new enhanced safeguards applicable to US intelligence gathering practices. As a result, the success of the DPF will be entirely judged on whether the US Government has managed to come up with a formula that makes its national security needs compatible with Europe's democratic values.

**It increases the options for transfer tools:** At a practical level, the DPF suddenly provides a more ample choice of mechanisms to legitimise transatlantic data transfers. Benefiting from the full swing of options available under the GDPR, transfers of data to the US can now be undertaken by fully relying on the DPF adequacy decision or by using any of the tools recognised by the law as adequate such as BCR or SCC. Essentially a choice between Article 45 and Article 46 for the connoisseurs. In reality, the applicable data protection standards should be the same. Relying on the DPF adequacy decision means that the US importer will have voluntarily joined the new DPF program which requires compliance with its GDPR-inspired principles, while the other methods bind the importer to follow more traditional versions of the same. Which one to go for is unlikely to be determined by how onerous the obligations might be but by what suits the culture, strategic thinking and practical priorities of the parties.

**TiAs haven't really gone away:** The biggest practical impact of the *Schrems II* decision was the requirement to undertake Transfers Impact Assessments (TIA) every time that a data transfer was legitimised through SCC or BCR. And while full reliance on the DPF does away with this requirement, transfers to the US which are subject to the safeguards provided by SCC or BCR will still need to be complemented by a TIA. However, the European Commission has done everyone a massive favour by undertaking a thorough assessment of the powers of US government agencies to access European data and firmly concluding that this is compatible with European law. So any TIA that considers the ability of existing SCC or BCR to protect data transferred to the US will be able to reach the same conclusion. Whether the same will be true for transfers to other countries is, of course, a different matter given the European regulators' strict approach to this issue.

**It will be scrutinised:** The only remaining question about the DPF that nobody can answer with absolute certainty is whether it will survive any eventual scrutiny by the Court of Justice of the European Union (CJEU). What is a lot more certain is that the appetite for that scrutiny remains, and while European regulators cannot directly challenge the validity of the Commission's adequacy decision, it only took 24 hours for Max Schrems himself to confirm that a legal challenge would be brought. As to the success of such a challenge, the truth is that anything can happen, but a fact that should not be ignored is that out of the 64 pages (excluding annexes) of the adequacy decision, nearly half of them are devoted to thoroughly assess the limitations and safeguards applicable to the access and use of personal data for national security purposes, as well as the oversight and redress mechanism. This is to say that beyond the political arguments and hyperbole, the legal analysis more than suggests that the DPF is robust, workable and lawful.



# EU: Prioritizing privacy under the EU AI Act

In this article, Sean Musch and Michael Borrelli, from AI & Partners, and Charles Kerrigan, from CMS London, explore the contents of the EU AI Act, the next steps for its implementation, and recommended best practices for companies to consider in order to remain compliant for the attention of data/information privacy professionals.



**Sean Musch** Co-CEO/CFO  
s.musch@ai-and-partners.com  
AI & Partners



**Michael Borrelli** Co-CEO/COO  
m.borrelli@ai-and-partners.com  
AI & Partners



**Charles Kerrigan** Partner  
charles.kerrigan@cms-cmno.com  
CMS London

## Key points

- European legislators' remain focused on the ethical application of artificial intelligence (AI).
- Negotiations on the final version of the EU AI Act began in July 2023.
- Firms should begin preparing for EU AI Act compliance with a code of conduct.

- Data/information privacy remains at the core of the EU AI Act.

## Understanding the EU AI Act

The EU AI Act<sup>1</sup> aims to regulate AI to ensure better conditions for the development and use of this innovative technology. It has been designed to make sure that AI systems used in the

EU are safe, transparent, traceable, non-discriminatory, and environmentally friendly, and to ensure that AI systems should be overseen by people, rather than by automation, to prevent harmful outcomes. In essence it:

- applies on a human centered risk-based approach





- classification of AI systems;
- applies to providers, users, importers, deployers, developers, and distributors of AI systems with an EU presence, direct or indirect; and
- is scheduled to take effect at the conclusion of the legislative process (expected at the end of 2023).

The EU AI Act sets down a legislative framework for dealing with AI in the future - with the goals of driving innovation and mitigating risks. It is about: emphasizing the ethical application of AI; instilling values improving transparency; establishing processes to enforce quality at launch and throughout the life cycle; fostering collaboration and a level playing field between EU Member States; and protecting the fundamental rights of EU citizens. No other regulation on AI has taken such a transformational approach

to achieving these goals. It sets an important precedent for years to come.

A regulation of this scale has to overcome certain barriers to implementation. The EU AI Act intends to achieve its ambitious goals by: incorporating a single standard across the EU to prevent fragmentation, enforced through Conformity Declarations and the obligation for a CE marking; providing legal certainty that encourages innovation and investment into AI by creating AI Regulatory Sandboxes; and enabling national competent authorities as controllers. These controllers will update an EU database for high-risk AI practices and systems. These are, of course, obligations that should be on the mind of C-suite executives across the globe to the extent they have an EU presence – customers, suppliers, or otherwise.

As the EU intends to lead the way with safe, secure, and trustworthy AI, it has put forward an entirely new body of law that aims to place ethical issues such as human oversight of automated machines at its core. To draw a parallel, the EU AI Act promises to have the same impact on interacting with AI as the General Data Protection Regulation (GDPR) had on personal data.

While the EU did not lead the world in AI, it is a pioneer in regulating and ensuring human-centered AI development, which is something that can give the EU an edge on AI innovation. The challenge for firms is in identifying how they are impacted by the regulation.

Any company based in, operating in, or otherwise servicing the EU, is affected by this EU AI Act. Even if

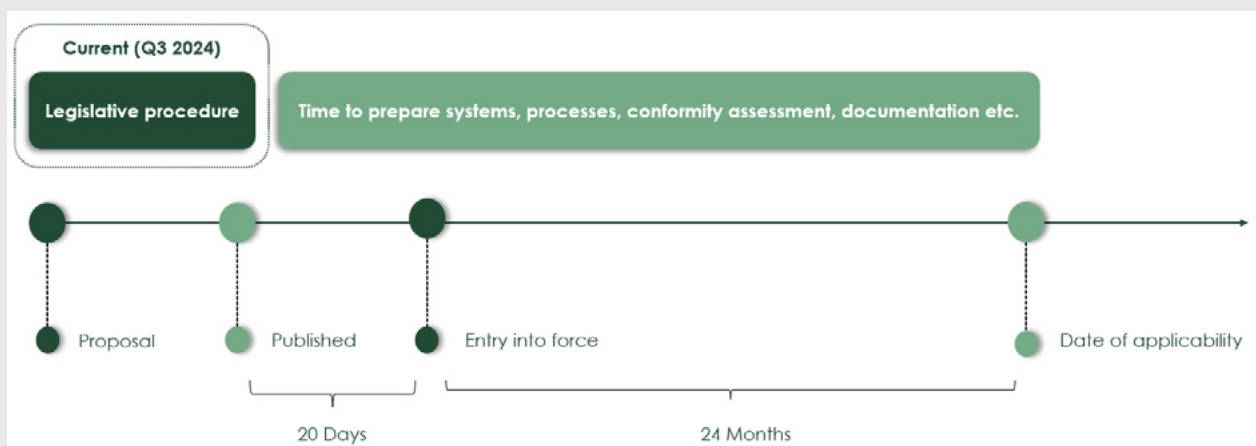


Figure 1. (AI & Partners, 2023)

the company is not developing an AI system itself, using systems that have an AI component present requires compliance with the new rules.

### Next steps for implementation

This is the continuation of an ongoing process on how AI should be regulated in the future. The next step that will shortly follow is for the EU AI Act to be negotiated by the European Council, the European Commission, and the European Parliament. Once completed, the regulation will come into force 20 days after its official publication in the EUR-Lex Journal of the European Union. Thereafter, it will apply from two years after that date. However, some provisions from the regulation will apply sooner. From the date of entry into force, it can be invoked by its subjects and will be enforceable.

### *It is necessary to track changes and automatically test whether or not AI systems remain compliant*

As shown in Figure one, we are currently in the latter stages of the legislative process whereby the latest version of the EU AI Act is being negotiated. The timeframe for firms may shift, yet the process has started. Once published, the European Commission remains responsible for ensuring national adoption and harmonization of the EU AI Act across individual Members States.

Firms should begin preparing for the EU AI Act now. Implementation is complex because the regulation is complex, contains many touchpoints to business operations, and the proposed fines are high.

Implementing AI systems should enable scalability, integration, and compliance from 'T+0.' Common structures in an organization ensure that the maintenance burden is as low as possible. Additionally, risk management leads to further adoption of the new tools.

### Best practices for compliance

Firms' governance mechanisms need to take steps to manage the risks related to AI systems, including that adequate controls are in place to comply with

adjacent regulations, relating to privacy, consumer, and non-discrimination.

### Code of Conduct

Title IX of the law relates to requirements for code of conduct. 'Those codes may also include voluntary commitments related, for example, to environmental sustainability, accessibility for persons with disability, stakeholders' participation in the design and development of AI systems, and diversity of development teams.'

For firms that are not familiar with setting up internal codes of conduct, there's an initial learning process. For firms familiar with setting up internal codes of conduct, this will be an easier journey. But existing frameworks that were not written for non-linear modelling or intelligent computer systems will lack the specifics that are needed to address the EU AI Act.

### Continuing obligations

The EU AI Act sets out the requirements (in Title I to XII) for high-risk models and ways to govern them:

- using high-quality training, validation, and testing data;
- using documentation and design logging features that ensure continuous documentation;
- ensuring transparency and informing users about the application of AI systems;
- ensuring human oversight throughout the process; and
- ensuring accuracy, robustness, and cybersecurity of systems.

With increasing regulation, it will become increasingly difficult to keep track of everything, in particular with systems that are dynamic. It is necessary to track changes and automatically test whether or not AI systems remain compliant.

### Data ethics

Data governance forms an integral part of the obligations that will apply to providers of high-risk AI systems. The Act requires providers to apply a range of measures to datasets that are used in the training, validation, and testing of machine learning and similar technologies. They include identifying potential biases, checking for inaccuracies, and assessing the

suitability of the data. The AI Act stresses privacy and absence of bias.

The AI Act builds on GDPR requirements applying rules on quality of datasets to ensure that biased models are not used. It is crucial to know what variables may affect the outcomes of a model including the weight each variable carries.

### Automatic documentation

It is necessary to document what is happening with any AI system and to track changes or updates. This includes code, systems, and decisions. Because machine learning is modifying the model through the learning cycle every time it retrains, it requires automated documentation.

Manual documentation would be quickly outdated. AI systems themselves must automatically generate necessary documentation to comply with requirements for continuous evaluation of AI system compliance.

Documentation is the core challenge in the process. In automated retraining, performance metrics must be reported automatically to a log. This is almost impossible to do manually, as the retraining process is also not manual and may not involve any human interaction.

### Firms can overcome privacy concerns

To summarize, the EU AI Act changes firms' interactions with AI. Adhering to privacy obligations under the EU AI Act remains essential. The key takeaways are:

- Risk-based approach: the treatment of AI systems under the EU AI Act depends on the risk category assigned.
- Limited transition period: following the publication of the EU AI Act in the official journal of the European Commission, firms have just over 24 months to put all measures in place. If the GDPR is an example of how this may unfold, firms should not take compliance lightly.

1. See: <https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence>



# GUIDE

# AI Playbook

**Understand your obligations and harness  
the power of artificial intelligence**

**Get to know global  
AI regulations**

**Empower AI system  
developers**

**Ensure responsible  
AI adoption**



**Get the guide**

**OneTrust DataGuidance™**  
REGULATORY RESEARCH SOFTWARE



# Germany: Getting to know the new whistleblowing legislation

*What is regulated? How does it differ from the EU Directive? What do Employers need to consider?*



**Tobias Neufeld** Partner  
tobias.neufeld@arqis.com  
ARQIS



**Sebastian Gutzeit** Legal Trainee  
sebastian.gutzeit@arqis.com  
ARQIS

With the introduction of the Whistleblower Protection Act (HinSchG) which came into effect on July 2, 2023, Germany finally implemented the EU Whistleblower Protection Directive. While the German legislation also hopes to improve the enforcement of rights on both a national and EU-wide level, its main objective is a different one. It has at its center the effective protection of the whistleblowers, previously a whistleblower could possibly be exposed to criminal prosecution, civil liability, termination of employment, or disciplinary proceedings. This protection is implemented by regulating the process of whistleblowing through reconciliation of the interests of all stakeholders all while standardizing the entire process of whistleblowing.

The Whistleblower Protection Act significantly expands the requirements of the EU Whistleblower Directive. Thus, whistleblowers are not only protected when reporting violations of EU law, but also when reporting violations of certain areas of national German law.

**What are the requirements under German whistleblowing legislation?**  
The Whistleblower Protection Act does

not have an applicability threshold, compliance therefore is required for every company operating in Germany as and when the Whistleblower Protection Act comes into force.

## **Scope of protection**

The material scope of application (Section 2 of the Whistleblower Protection Act) includes reports of violations of laws with criminal penalties that the respective company must comply with (e.g. labour law, criminal law) as well as violations of laws and regulations imposing a fine that serve to protect life, limb or health or the rights protecting employees or their representative bodies (e.g. environmental law, data protection, occupational health and safety laws) committed in the course of a professional, business, or official activity, if the reports are committed in 'good faith.' The motivation of the whistleblower is not relevant for the protection under the Whistleblower Protection Act, meaning even if the whistleblower reports the incidence just for personal gain or out of selfish motives it remains applicable. The 'good faith' requirement need only apply to the truthfulness of the report made.





The personal scope of application encompasses all employees and business partners (Sections 1, 3 VIII, 34 of the Whistleblower Protection Act) with a 'work related connection.' A 'work-related connection' to the respective company can include active and former employees, applicants, trainees, apprentices, temporary workers, and other persons similar to employees, business partners, and suppliers. In addition, the confidants of these protected group also fall within the Whistleblower Protection Act themselves. This extensive approach, with the broad general clause, is directly from the European law.

Whistleblowers obtain comprehensive protection by means of a legal prohibition against discrimination and reprisals (e.g., warning, reassignment, dismissal, or similar) in connection with their report (Sections 3 VI, 36 ff of the Whistleblower Protection Act) in case of violation, damages may be claimed. This protection is further strengthened by a reversal of proof of burden, in case of dispute it is up to the employer to prove that they have not subjected the whistleblower to undue reprisals or discrimination as a result of the report.

#### **Options of whistleblowing**

Reports may be submitted equally to a company's internal reporting system or to an (official) external reporting office. The main and central online reporting point has been opened at the Federal Ministry of Justice. In addition, there are several other specialized online reporting points (e.g., the Federal Financial Supervisory Authority, the Federal Cartel Authority).

As a secondary form of whistleblowing, the Whistleblower Protection Act also

includes the option of public disclosure (Section 32 of the Whistleblower Protection Act). In this case the whistleblower shall only be protected if their previous report to an external reporting office was unsuccessful or the whistleblower had reasonable grounds to believe: (i) a threat to the public was imminent or comparable circumstances; (ii) in the event of an external report reprisals are to be feared; or (iii) the suppression of evidence or collusion between the responsible company and the external reporting office are to be feared.

From July 3, 2023, an internal reporting system must be in place for private sector companies larger than 249 employees. Starting December 17, 2023, this internal reporting system must also be in place for companies smaller than 249 and larger than 50 employees. Starting from December 1, 2023, a fine of up to €20,000 can be imposed for non-implementation of an internal reporting system.

#### **Legal requirements of the internal reporting system**

The companies required to implement an internal reporting system have different options on how to comply with the Whistleblower Protection Act. Internal reporting systems may be implemented by entrusting: (i) a person employed at the company; (ii) a work unit consisting of several employed persons; or (iii) a third party. The chosen option of an internal reporting system must be accessible for all employees. As mentioned above, the scope of employee is wider than just current employees as it includes all possible whistleblowers with a work-related connection. The system must

make both oral and written and reports possible, and additionally an in-person meeting if the whistleblower so desires.

***Employers are now under the challenge to not only comply with this new German whistleblowing legislation, but also to navigate the pitfalls...***

Strict confidentiality with regard to not only the whistleblower's identity but also to the identity of the suspected persons and witnesses must be upheld. The duty of confidentiality applies to each and every incoming report regardless of whether the point of reporting is responsible for the receipt of the incoming message. For this reason, it is crucial that only the persons authorized to receive the reports under ordinary circumstances have access to incoming reports. If a supporting party has to be consulted for support, access may only be permitted within the scope of the support activity and only to the extent necessary for the support activity. All reports should therefore only be made available to the respective person based on a need-to-know principle. It is worth noting that while anonymous reports should be processed according to Section 16 of the Whistleblower Protection Act, a legal obligation within the Act however does not exist.

In addition to the procedural and access requirements, the Whistleblower Protection Act requires the companies under the burden of implementing an internal reporting system to comply with a documentation duty. This duty entails documentation of all incoming reports in a permanently retrievable way. In

the case of telephone reports or voice transmissions, this can mean permanently retrievable audio recording or a verbatim record. However, this is permitted only with the consent of the whistleblower. Alternatively, a content record by the receiving person is a veritable possibility to comply with the documentation requirements. In case of a requested in-person meeting, the company must keep a reviewed and confirmed protocol signed by the whistleblower.

## **The Whistleblower Protection Act significantly expands the requirements of the EU Whistleblower Directive**

Companies must ensure the documentation of the necessary reports are securely stored for at least three years after the case is closed. Reports may be kept for longer periods of time if this is deemed necessary and proportionate. In all cases, the company under an obligation to delete these reports after the documentation time period is elapsed.

### **Processing of internal reports**

In order to streamline and standardize the response to internal reports, in Section 17 of the Whistleblower Protection Act, the legislator has imposed mandatory procedural requirements for the processing of internal reports.

After an internal report is filed, the whistleblower must receive a confirmation of receipt of the report within seven days of their report. Subsequently, the responsible body within the company is under a duty to verify whether the reported non-compliance falls within the scope of application under Section 2 of the Whistleblower Protection Act. During this verification process, the responsible body shall maintain contact with the whistleblower and, if necessary, request further information. After the initial verification, an assessment of the validity of the reports of non-compliance is to be conducted. Subsequently to the verification, the responsible body in any case has to carry out adequate follow-up measures. These follow up measures may include the launch of an internal investigation, the referral to a competent authority, public prosecutor, or a dismissal.

To comply with Section 17 of the Whistleblower Protection Act, the responsible body must notify the whistleblower within three months of the confirmation of receipt of the report of any follow-up measures already taken and, if applicable, planned follow-up measures, as well as the reasons any

measures were taken. Any feedback to the whistleblower may only be made to the extent that it does not affect any internal enquiries or investigations and does not infringe the rights of the persons who are subject of or named in the report.

### **What employers need to address**

Employers are now under the challenge to not only comply with this new German whistleblowing legislation, but also to navigate the pitfalls, especially with regard to data protection, all while optimizing the opportunities and utilizing synergies under this new body of law.

### **Whistleblowers and the GDPR**

As the Whistleblower Protection Act is not exempt from the General Data Protection Regulation (GDPR), the employers obliged to implement an internal reporting system must ensure that their system is compliant with data protection principles. Therefore, the system must be lawful, fair, and transparent, the data processing must be purpose limited and minimized, and any data processed must be accurate. In addition, the internal reporting system must not store the data for unlimited amounts of time and must be secure and able to maintain confidentiality.

### **Duty to inform the data subject under Article 14 of the GDPR**

When a report is received, personal data might be collected without the knowledge of the data subject. Thus, the employer would be obliged to inform the data subject comprehensively under Article 14 of the GDPR about the collection and processing of the data, in particular about the purposes and the source of the information. Employers would have to disclose both the content of a report and the identity of the whistleblower on their own initiative, especially since a violation of the duty to inform is subject to a fine (Article 83(5)(b) of the GDPR). Nonetheless, the provision of information about the whistleblower directly contradicts the obligation to ensure confidential handling of the whistleblower's data. The provision of information on the content of a report can also impair the success of internal investigations. The Whistleblower Protection Act does not resolve this tension. Only the explanatory memorandum refers to Section 29(1) of the Federal Data Protection Act (BDSG), according to which the duty to inform does not exist by way of exception, insofar as its fulfilment would disclose information which by its nature must be kept secret, in particular because of the overriding legitimate interests of a third party. With regard to the content of a notification, the exception in Article 14(5)(b) of the GDPR may also apply. According to this provision, the obligation

to provide information does not exist if it is likely to make the achievement of the objectives of the processing impossible or seriously impair it. Nonetheless, in the course of processing notifications, the duty to inform may 'revive' for certain data if the employer's interest in secrecy no longer prevails. Therefore, employers should comply with the duty to inform at the latest after securing the relevant evidence in the course of an initial interview with the accused.

### **Subject access request under Article 15 of the GDPR**

In case of persons who are the subject of an expressed suspicion, there is also the right to access to information pursuant to Article 15 of the GDPR which can conflict with the Whistleblower Protection Act: This right includes, among other things, information about the origin of the data (Article 15(1)(g) of the GDPR) and a violation of the duty to provide information might be subject to a fine (Article 83 of the GDPR). If this right is granted without restraints, the suspect would have a veritable option to find out the identity of the whistleblower. In the absence of an explicit provision in the Whistleblower Protection Act, a balance of the conflicting interests can only be found on the basis of the exception provision in Section 29(1) of the BDSG: According to this provision, the right to information does not exist if the information disclosed must be kept secret according to a legal provision or by its nature. With a view to the confidentiality requirement under the Whistleblower Protection Act, it can be argued that this such a legal provision, not only entitles but also obliges the employer to refuse a request for information by the suspect.

### **Implementation of the internal reporting system**

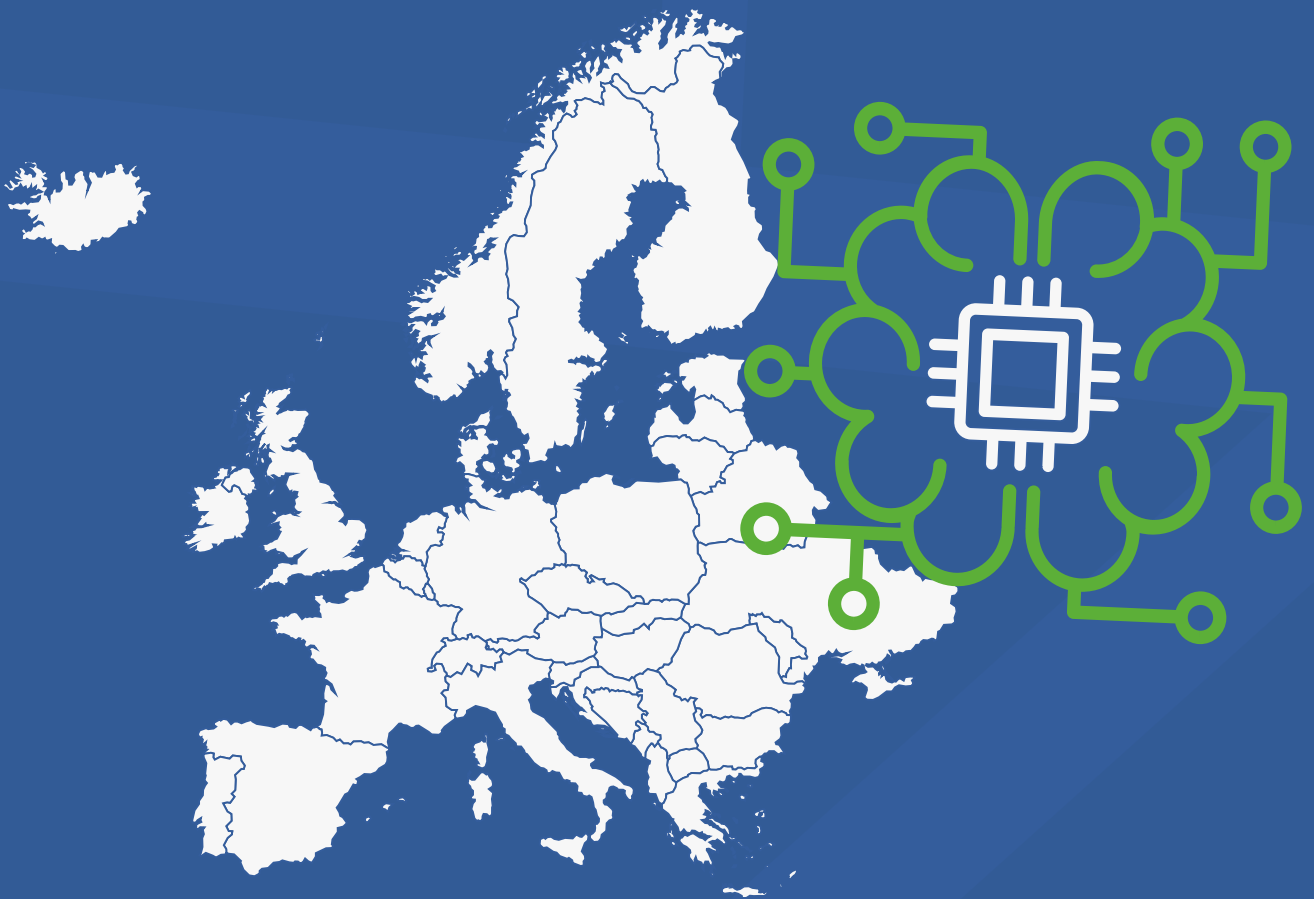
Before any implementation of an internal reporting system, a Data Protection Impact Assessment is mandatory to comply with Article 35 of the GDPR as the data processing to be carried out with the internal reporting system is likely to present a high risk to the rights and freedoms of natural persons.

In addition, German labour law grants participating rights to a works council – if one is elected in the employing company – before the implementation of an internal reporting system under Section 87 of the Works Constitution Act (BetrVG). It would also be beneficial for the employers to consider the requirements for the complaints procedure according to the Supply Chain Obligations Act (LkSG) in order to utilize synergies and optimize inter reporting processes.



Unpacking Digital Data  
Laws Across Europe

# The EU's AI Act and Developing an AI Compliance Program



Watch on demand

# GDPR Fine Enforcement: Q2 2023 Report

April 1, 2023 - June 30, 2023

## Quarterly Enforcement Highlights

### Total Fines Issued

€ 1,267,085,407.00

### Largest Singular Fine



1.2B€

Irish DPC issued €1.2 billion fine to Meta for unlawful US data transfers

Fine

15M+

### Most Enforcements



Spain

accounted for 54% of enforcements with 98 total

Fine amount (€)

10M

5M

### Most Frequently Enforced

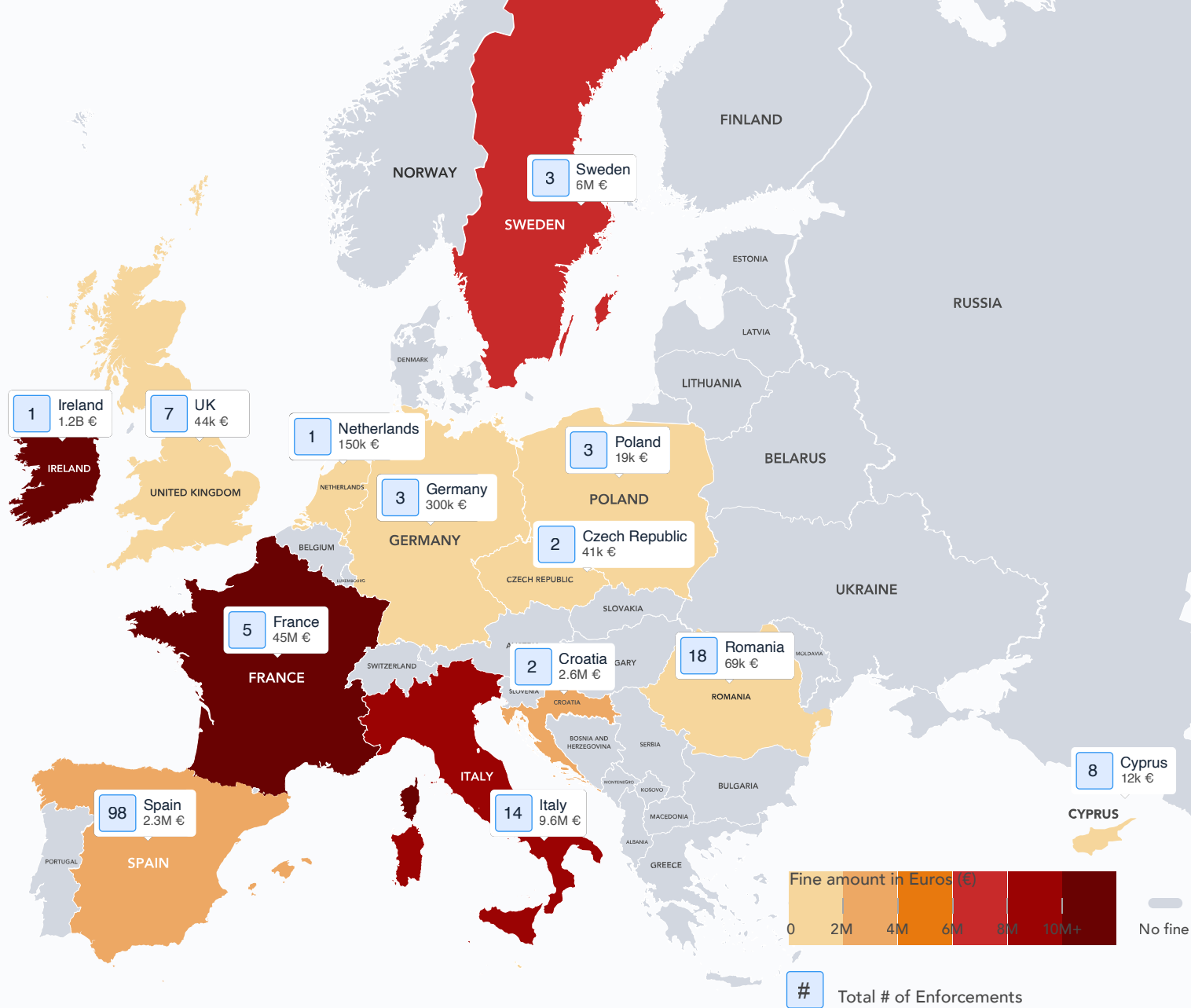


Legal basis for processing

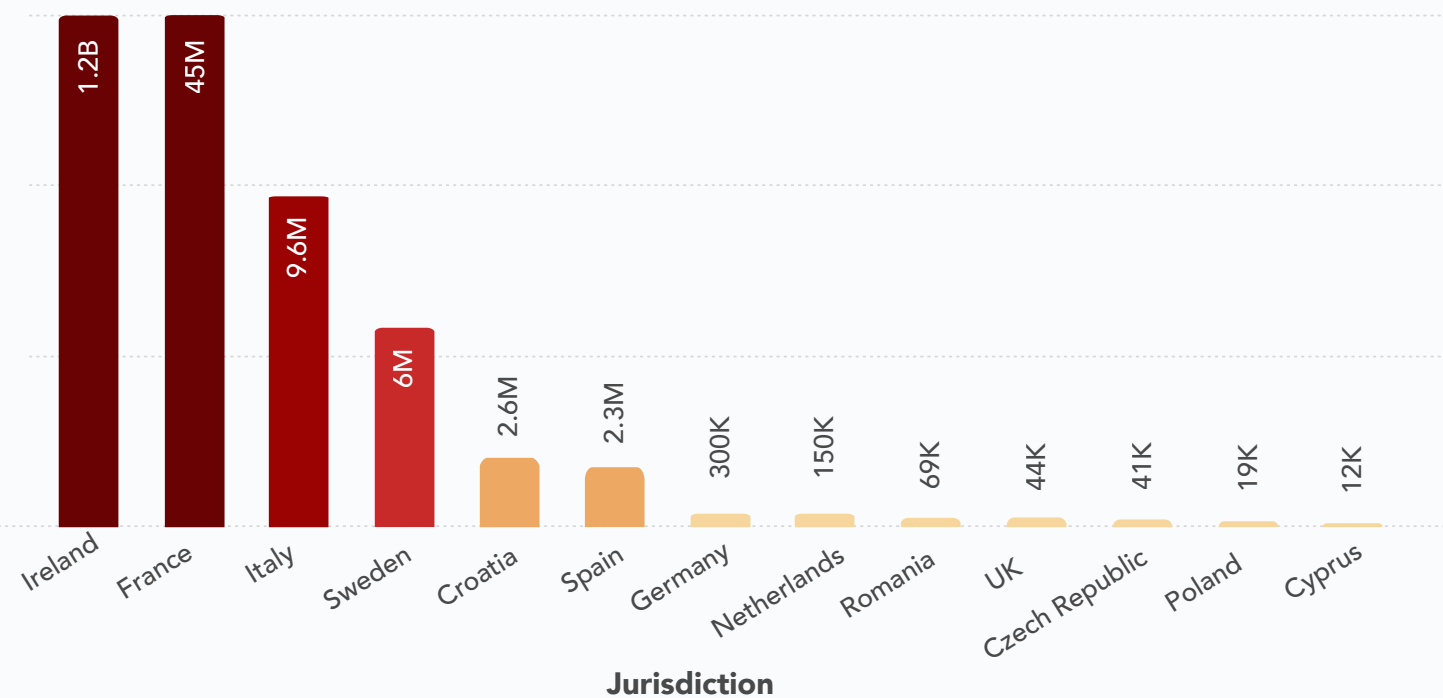
accounted for 29% of all enforcements issued

0M





## Amounts by Jurisdiction





# Meet a DPO:

## Fabrizio Venturelli, Global DPO at Workday



*Tell us about yourself and your role. How would you describe it and what does a 'typical' day look like?*

The office of the DPO at Workday plays an oversight and independent role in order to monitor GDPR compliance across the organization. That is probably the most interesting part: the breadth of projects and topics we are involved in makes every day different from the other.

I lead the office of the DPO and report to the Chief Privacy Officer (CPO); we are part of the Legal Compliance and Corporate Affairs function managed by the General Counsel.

Being the DPO, an oversight function, a big part of it is about

building relationships and opening communication channels with the right stakeholders in order for us to be kept in the loop in important conversations about data protection. In addition, giving advice, assessing privacy risk, overseeing projects and coordinating with different teams, from the Legal, to the HR, to Safety and Information Security are crucial for my role. Being a DPO allows you to collaborate proactively with many different teams at Workday.

*What drew you to working in data protection and privacy?*

I have a legal background, I've trained as a magistrate, but my interest has always been with new technologies, and when I got my Master of Law, in 2009/2010, social media was about to become really popular. That's when I decided to combine my studies with my passion and privacy seemed to be a great link among the two things. So, I started to cultivate the idea to become, one day, a DPO for a tech company. First, I wrote my dissertation on social media and data protection in EU and US legal systems. Then, I worked for a while in law firms, online banking cloud

providers, outsourcing multinationals, and eventually I joined Workday, relocating to Ireland from Italy.

*What are the key privacy compliance areas that are top of mind for you right now for your program?*

Cross-border data transfer is definitely an important area to monitor; Workday received approval for Processor Binding Corporate Rules and for APEC Privacy Rules for Processors. In addition, our Master Subscription Agreement includes EU Standard Clauses.

We also partner with our global customers when they have to perform any Transfer Impact Assessment. In this regard, we fully support the new EU-US Data Privacy Framework; the adequacy decision provides our customers with greater certainty that European personal data can legally be transferred to the United States.

Another key topic is data privacy regulations that vary across regions and countries. We monitor evolving requirements where Workday operates, and based on

our assessment, we adapt our operational practices. In addition, as requirements also vary based on customers (depending on the industry, types of data, policy commitments etc.), we're ready to support them to understand how our program supports their compliance needs.

Last but not least, artificial intelligence (AI). Workday believes that AI functionalities and privacy protection are not mutually exclusive. Proper data privacy measures can actually help build trust and confidence in AI and machine learning (ML).

We are not reinventing the wheel; we leverage our history of Privacy by Design principles in the development and management of our ML governance program. For example, our teams partner on data minimisation; another cross-functional group works in order to ensure data processed is absolutely necessary; after data collection begins, data that's no longer necessary is removed.

***What are the key elements of your privacy program? Is it based on particular laws/standards/frameworks? How has it evolved over time?***

We constantly monitor the ever-changing regulatory landscape based on the regions where Workday operates and our customer needs. In addition, to demonstrate compliance, we maintain our SOC2 Report and ISO Certifications. We have also been the first company to certify adherence to the EU Cloud Code of Conduct. Finally, as AI is becoming a leading trend in

the industry, we also supported and contributed to the National Institute of Standards and Technology's AI Risk Management Framework.

***We monitor evolving requirements where Workday operates, and based on our assessment, we adapt our operational practices***

***Which other business functions do you regularly interact with, and why?***

In addition to the broader Legal team, and Information Security, the office of the DPO is involved with the teams that develop our software, in order to embed privacy requirements in our product from the scratch.

We also work together with corporate functions when it comes to our internal practices. In general, we aim to build recurrent touch points with most of the relevant functions, creating channels for ad-hoc escalations when needed.

***What advice would you give to others looking to maintain and evolve their privacy programs?***

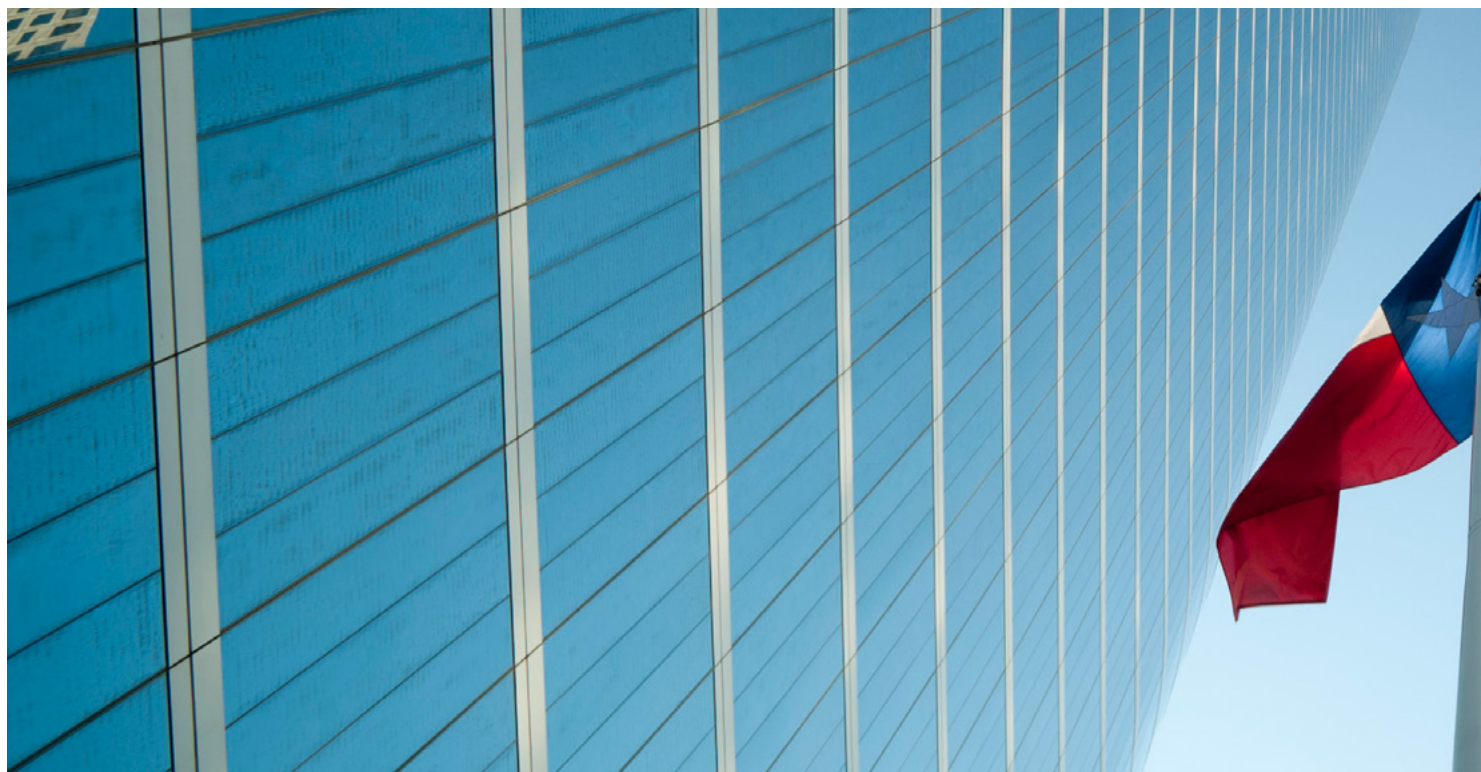
I would monitor the changing laws, but at the same time I would set up a principle-based global privacy program. Which doesn't mean a one-size-fits-all approach, but a system that allows to monitor and oversee the most important privacy related risks and prioritize them in the context of a framework.

In addition, I would invest into keeping the privacy team, and in

particular the DPO, independent and assigning clear roles and responsibilities across the functions.

Last but not least, certifying for relevant frameworks such as SOC, ISO, Codes of Conduct, may help in demonstrating compliance externally, but also to streamline assessments internally.





# State Profile: Texas

## *Texas joins the privacy rodeo with new consumer data privacy law and social media law*



**Bart Huffman** Partner  
bart.huffman@hklaw.com  
Holland & Knight LLP



**Haylie Treas** Associate  
haylie.treas@hklaw.com  
Holland & Knight LLP<sup>1</sup>

Texas has joined a number of other other U.S. states in passing a comprehensive data privacy law, the Texas Data Privacy and Security Act<sup>2</sup> (TDPSA). The TDPSA has many things in common with the data privacy laws in other states, but there are also some notable differences.

An important theme of the TDPSA is transparency – companies should limit their collection of personal data to what is 'adequate, relevant, and reasonably necessary' and should not process such data for a purpose that is not reasonably necessary or compatible with the disclosed purpose<sup>3</sup>.

For similar as well as safety concerns, the Texas legislature also passed a child-protective social media law, the Securing the Children Online through Parental Empowerment Act<sup>4</sup> (the SCOPE Act), which is similar to that passed by some other states (Utah and Arkansas). According to the House Committee Report for the SCOPE Act, in drafting the act, the Texas legislature considered that:

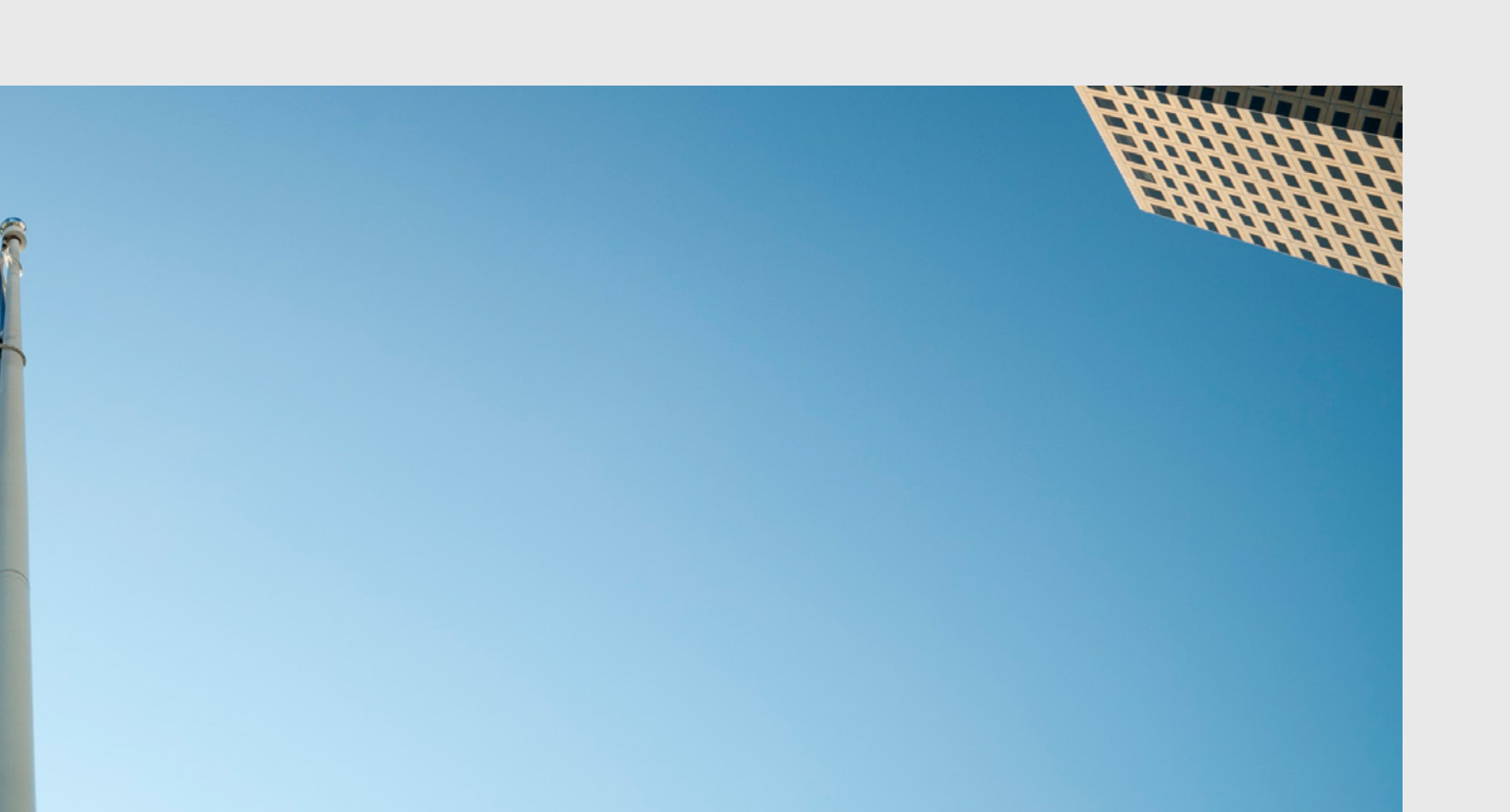
'Mounting evidence draws a strong connection between uninhibited access to social media platforms and online content and the harmful consequences of such access—this is especially true for children...In tandem, platforms are collecting and processing vast amounts of data from minors. This data raises privacy concerns and feeds algorithms that fuel online addiction'<sup>5</sup>.

Accordingly, the SCOPE Act imposes strategic safety planning obligations on certain social media providers and gives parents and guardians rights to be involved and exercise oversight.

### **Who must comply?**

#### **TDPSA**

Any person that: (i) conducts business in Texas or produces products or services consumed by a Texas resident; (ii) processes or engages in the sale of personal data; and (iii) is not a small business is subject to the TDPSA<sup>6</sup>. Interestingly, the TDPSA on its face would apply to an otherwise-qualified company that merely 'produces' any goods or services that are 'consumed'



by Texans – that threshold seems much lower than the 'doing business' requirement under other state privacy laws. As for the size requirement, a 'small business' is not really that small (as a general rule, more than 500 employees, with other thresholds that are in the millions of dollars in revenue and/or involve hundreds of employees), so a broad swathe of the economy is not subject to the TDPSA. Notably, even a 'small business' must still comply with the requirement to obtain consent prior to selling sensitive personal data<sup>7</sup>.

In addition to the jurisdictional breadth, the scope of the TDPSA appears to cast a broader net than other U.S. privacy laws. The TDPSA uses language that extends to 'produc[ing] a product or service consumed by residents of' Texas<sup>8</sup>, rather than producing a product or service that is 'targeted to residents' of the state<sup>9</sup>. The Texas applicability provisions are also broader in scope than most other U.S. state privacy laws (such as Virginia) in that Texas does not include a minimum number of consumers whose personal data must be processed in order to cross the threshold.

In effect, then, good-sized companies located anywhere who have any customers in Texas should carefully consider compliance (absent a desire to challenge the statute's applicability on personal jurisdiction grounds), unless the company is in a

category that is exempt under other provisions (e.g., non-profits, financial institutions, HIPAA-covered entities, institutions of higher education, state agencies, utility providers, etc.).

#### **The SCOPE Act**

The SCOPE Act extends to any 'digital service provider' that provides the following services: (i) connects users and allows them to socially interact; (ii) allows a user to create a public or partially public profile for the purpose of using the service; and (iii) allows a user to create or post content that can be viewed by other users, such as on a message board, in a chat room, or on a video channel<sup>10</sup>.

According to a statement of legislative intent, the SCOPE Act was enacted in support of a reasonable duty of care to prevent minors from being exposed to harmful content, such as abuse, exploitation, and enticement<sup>11</sup>.

Notably, the SCOPE Act exempts digital service providers whose primary function is to 'provide a user with access to news, sports, commerce, or content primarily generated or selected by the digital service provider' and allows chats and comments as an incidental part of the service<sup>12</sup>. Like the TDPSA, the SCOPE Act does not apply to certain types of entities, including a 'small business[es],' state agencies, financial institutions, and HIPAA-covered entities, etc<sup>13</sup>.

***Companies doing business in Texas, including providing products or services to those in Texas, should begin evaluating whether they are or may soon be within the scope of the TDPSA***

#### **What do the new laws cover? TDPSA**

##### **Consumers only**

Like the privacy laws in Virginia, Colorado, Connecticut, and Utah, the TDPSA does not apply to data of job applicants, employees, and independent contractors to the extent the data is collected in the employment context (including to administer benefits)<sup>14</sup>. The TDPSA also does not apply to business-to-business information<sup>15</sup>.

##### **Consumer rights**

As under the other U.S. state privacy laws, the TDPSA provides consumers with the following rights:

- to access the consumer's personal data;
- to correct inaccuracies in the personal data;
- to delete personal data (with exceptions);
- to obtain a copy of the personal data if it is available in a digital format; and
- to opt out of processing for the

purposes of targeted advertising, the sale of personal data, or 'profiling in furtherance of a decision that produces a legal effect of similarly significant effect concerning the consumer'<sup>16</sup>.

***[T]he SCOPE Act imposes strategic safety planning obligations on certain social media providers and gives parents and guardians rights to be involved and exercise oversight***

A consumer also has the right to not be discriminated against for exercising their rights under the TDPSA<sup>17</sup>. A company must respond to a consumer's request without undue delay and not later than 45 days after the request is received<sup>18</sup>.

If a company refuses the consumer's request, the consumer has the right to appeal the refusal and the appeal process must be conspicuously available and similar to the process of submitting the request in the first place<sup>19</sup>.

While the TDPSA does not prescribe specific methods that must be provided for submitting consumer requests (unlike the Californian privacy law and its toll-free number requirement), the TDPSA does require that a company establish two or more methods to submit a request<sup>20</sup>.

The TDPSA allows for the use of authorized agents, but only under limited circumstances. A consumer may designate an authorized agent to exercise a right to opt-out of selling personal data or processing personal data for targeted advertising<sup>21</sup>.

The TDPSA contemplates the use of authorized technology agents (including global privacy controls): 'A consumer may designate an authorized agent using a technology, including a link to an Internet website, an Internet browser setting or extension, or a global setting on an electronic device, that allows the consumer to indicate the consumer's intent to opt out of the processing'<sup>22</sup>.

#### **Consent requirements**

Before processing sensitive personal

data (including data that reveals racial or ethnic origin, mental or physical health diagnosis data, biometric data, data of a known child, or precise geolocation data), a company must obtain consent<sup>23</sup>. This is consistent with the trend in other states (except for California, which includes protected identifiers such as Social Security numbers in its broad definition of sensitive personal data).

#### **Privacy notice**

A company must provide clear a privacy notice that describes:

- the categories of personal data processed;
- the purpose of processing;
- the manner in which consumer rights can be exercised; and
- the categories of personal data shared with third parties and the categories of those third parties<sup>24</sup>.

Also, if the company sells sensitive personal data or biometric data, the company must include a specific statement in the privacy notice ('NOTICE: We may sell your sensitive personal data' or 'NOTICE: We may sell your biometric personal data')<sup>25</sup>.

In addition, the company must clearly describe the process that the consumer can use to opt out of such processing<sup>26</sup>.

#### **Service providers (processors)**

Service providers are required to assist with responding to consumer requests, complying with security requirements, and providing information needed by the company to perform Data Protection Assessments (DPAs)<sup>27</sup>. In addition to this, the company must also enter into a written contract with the service provider that contains specific provisions, including limited processing of data and audit requirements<sup>28</sup>.

#### **DPAs**

If a company processes personal data for the purpose of targeted advertising, sells data, or processes personal data for the purpose of foreseeably risky profiling, the company must conduct a DPA<sup>29</sup>.

This may be a broad requirement. And, if the Texas Attorney General (AG) issues a civil investigative demand, a company's DPA must be provided (but, importantly, the assessment will still be treated as confidential and is exempt from public records act disclosure)<sup>30</sup>.

#### **The SCOPE Act**

##### **Age collection**

A digital service provider covered by the SCOPE Act must collect the age of any person wanting to create an account<sup>31</sup>.

##### **Limited data collection and use**

A digital service provider must limit its collection and use of personal data from a known minor<sup>32</sup>.

The digital service provider is prohibited from:

- allowing a known minor to make purchases or financial transactions through the service;
- sharing, disclosing, or selling the known minor's personal data;
- using the service to collect precise geolocation data of a known minor; and
- using the service to display targeted ads to known minors<sup>33</sup>.

##### **Duties of digital service providers**

A digital service provider has a heightened duty to protect minors, with substantial, express obligations.

The provider has a duty to prevent harm to known minors and must:

- develop and implement a comprehensive strategy to prevent exposure to material that promotes harmful behavior;
- create parental tools to allow verified parents or guardians to supervise a known minor's use of the service; and
- make commercial reasonable efforts to prevent advertisers on the service from targeting known minors with certain advertisements<sup>34</sup>.

##### **Use of algorithms**

To the extent algorithms are used on the service (including especially algorithms used to prioritize or filter content delivered to known minors), the digital service provider must explain the algorithm(s) in its terms of service, privacy policy, or similar document<sup>35</sup>.

##### **Tools for parents or guardians**

Verified parents have the power to modify the duties of digital service providers with respect to their child, may exercise access and deletion rights with respect to the child's personal data, and are entitled to use supervisory tools that must be provided by the digital service providers<sup>36</sup>. The digital service



provider must include functionality to enable all this parental oversight.

### Who enforces the laws and when are they effective?

Both laws are enforced by the Texas AG and do not include a private right of action<sup>37</sup>. However, the SCOPE Act provides that a parent or guardian of a minor may bring a cause of action against a digital service provider seeking a declaratory judgment or injunction if they believe a minor is affected by the digital service provider's violation of the act<sup>38</sup>.

The TDPSA allows for a 30-day cure period<sup>39</sup>. Violations of the law may trigger fines of up to \$7,500 for each violation<sup>40</sup>.

The TDPSA is effective from July 1, 2024, except that the section relating to authorized agents exercising rights on behalf of the consumer (including global privacy controls)

will not become effective until January 1, 2025<sup>41</sup>. The SCOPE Act is effective from September 1, 2024<sup>42</sup>.

### Next steps

Companies doing business in Texas, including providing products or services to those in Texas, should begin evaluating whether they are or may soon be within the scope of the TDPSA. Even business-to-business companies may have some compliance obligations in relation to data collected from consumers via their websites.

Digital service providers that are subject to the SCOPE Act should begin developing a plan to comply with the law. Notably, because the law requires the collection of age information, digital service providers will have actual knowledge of the ages of all users, even those under 13 years old. The overall exercise by digital service providers should be undertaken in connection with

compliance with children's privacy laws, including the Children's Online Privacy Protection Act.

1. Please don't hesitate to reach out to the authors with any comments about this article or its subject matter.  
2. See: <https://capitol.texas.gov/tlodocs/88R/billtext/pdf/HB00004F.pdf>  
3. Tex. Bus. & Com. Code § 541.101.  
4. See: <https://capitol.texas.gov/tlodocs/88R/billtext/pdf/HB00018F.pdf>  
5. <https://capitol.texas.gov/tlodocs/88R/analysis/pdf/HB00018H.pdf>  
6. Tex. Bus. & Com. Code § 541.002.  
7. Id. at § 541.002(a)(3).  
8. Id. at § 541.002(a)(1).  
9. See e.g. Va. Code Ann. § 59.1-576(A).  
10. Tex. Bus. & Com. Code § 509.002(a).  
11. See: <https://journals.house.texas.gov/hjrn/88r/pdf/88RDY48FINAL.PDF>  
12. Tex. Bus. & Com. Code § 509.002(a)(10)(A).  
13. Id. at § 509.002(b).  
14. Tex. Bus. & Com. Code §§ 541.001(7), 541.002(a)(15)-(17).

15. Id. at § 541.001(7).  
16. Id. at § 541.051(b).  
17. Id. at § 541.101(b)(3).  
18. Id. at § 541.052(b)-(c).  
19. Id. at §§ 541.052(c), 541.053(b).  
20. Id. at § 541.055.  
21. Id. at § 541.055(e).  
22. Id.  
23. Id. at § 541.101(b)(4).  
24. Id. at § 541.102.  
25. Id. at § 541.102(b), (c).  
26. Id. at § 541.103.  
27. Id. at § 541.104(a).  
28. Id. at § 541.104(b) (contract must include, among other things, cooperation with assessments or the provision of an independent assessment, downstream contracting obligations as to subcontractors, and a means for oversight as to any shared pseudonymized or deidentified data).

29. Id. at § 541.105(a) (assessment required for targeted advertising, profiling with a foreseeable risk of various potential harms, and processing of sensitive data).  
30. Id. at § 541.105(c)-(d).  
31. Tex. Bus. & Com. Code § 509.051(a).  
32. Id. at § 509.052(1).  
33. Id. at § 509.052(2).  
34. Id. at §§ 509.053, 509.054(a), 509.055.  
35. Id. at § 509.056.  
36. Id. at §§ 509.102, 509.103(a), 509.054.  
37. Tex. Bus. & Com. Code §§ 541.151, 541.156, 509.151, 509.152.  
38. Id. at § 509.152(b).  
39. Id. at § 541.154.  
40. Id. at § 541.155.  
41. Texas Data Privacy and Security Act, Sec. 7, H.B. 4, 88th Leg., Reg. Sess. (Tex. 2023).  
42. Securing the Children Online through Parental Empowerment Act, Sec. 5.03, H.B. 18, 88th Leg., Reg. Sess. (Tex. 2023).



# Five years of GDPR: what is the best way to approach new digital challenges



**Robb Hiscock** OneTrust Editorial Team  
rhiscock@onetrust.com

When I look back to my first interactions with the GDPR, I remember being inundated with requests for my consent to remain on mailing lists and to receive marketing materials from what seemed like every company on the planet. It was plain to see that, among other things, the GDPR was being developed off the back of a rapid rise in personal data being collected and used by organizations for targeted advertising and other lucrative activities. Remember, when the Regulation was first introduced at the beginning of 2012, a pre-IPO Facebook was (only) worth an estimated \$83.5 billion<sup>1</sup> and Instagram was a mere two years old - both a far cry from the social media and digital advertising behemoths they are today. In the face of this accelerated technological advancement, the GDPR would have the initial goals of addressing individuals' awareness of their new data protection rights, modernizing the Data Protection Directive 1995, and consolidating data protection efforts across the EU.

In this respect, you could argue that the GDPR has been a success. It has held businesses to account through strict

requirements for using personal data, raised general awareness of personal data protection across the world, and has handed out several significant fines for those that haven't followed the rules. However, challenges on the horizon such as AI and data transfers should make us pause and consider how we might move forward from here. If we were to start discussing GDPR reform, we would need to have a deep understanding of the driving factors that would make it a viable option and question whether a reformed GDPR would even be able to tackle the challenges that we are set to be presented through ongoing digital development. Or, should lawmakers in the EU approach each new challenge with targeted and specific regulations, much like the incoming suite of digital regulations?<sup>2</sup>

This suite of digital regulation in the EU certainly looks to be creating a solution for some of the broader issues that our ever-evolving digital landscape is throwing at us. Many of the acts within this suite of legislation specifically call upon the GDPR and aim to interact with, and enhance, its requirements. For example, the AI Act – which has been developed to allow businesses to innovate with new technologies but in a manner that is secure, ethical, and trustworthy<sup>3</sup> – will seek to ensure additional protection for personal data that will apply in addition to the GDPR where AI and similar systems are processing personal data. Taking the approach of building on top of, and interacting with, the GDPR with technology, or scenario-specific regulations, certainly allows legislators to make targeted action in

areas of concern and react to them with a degree of urgency. What this also suggests is that the GDPR remains fit for its intended purpose and can continue to serve a valuable basis that underpins new and future digital regulation for some years to come.

Many might dismiss the thought of the GDPR requiring any form of major revamp, after all it has only been enforceable for five years and how much can we read into its effectiveness in that space of time? Equally, there are critics of the GDPR that would argue – in some cases vehemently – that the GDPR needs a significant overhaul. Take the United Kingdom for example. Once under the purview of the EU GDPR but quick to propose reform in the aftermath of Brexit, the UK Government has attempted to modernize the data protection law in the jurisdiction by delivering its own “pro-growth” and “innovation-friendly” version of the GDPR. But it seems that the EU's attempts to create a patchwork of digital regulations could further propel the region as a vanguard in managing our data-driven society and might just be the answer we need for approaching new digital challenges and in some cases enhance the protections that the GDPR currently offers.

As with most things in life, there will always be imperfections to be found in any proposal, law, or regulation but it is with the constant scrutiny of these imperfections that we can attempt to move towards a digital landscape governed by rules that do right by the individual – no matter what approach we take to achieve it.

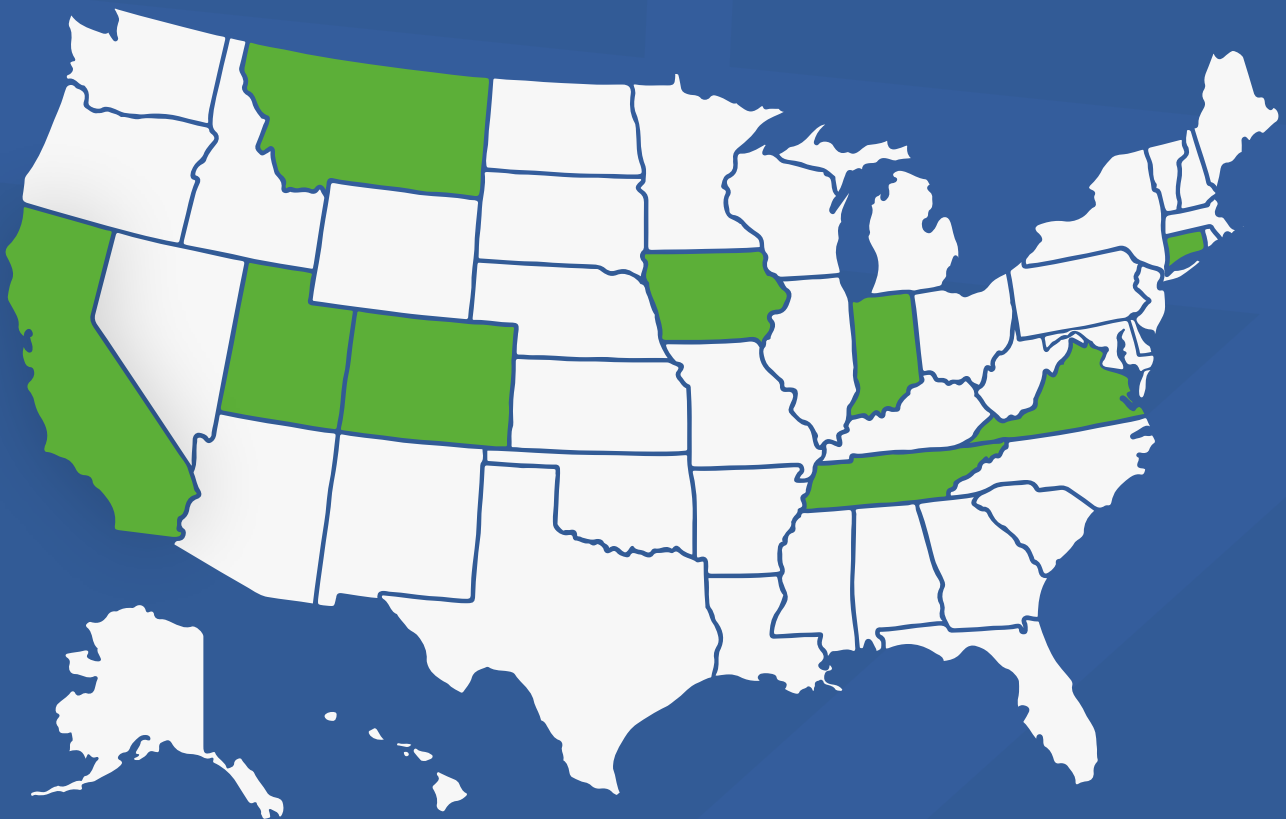
1. See: <https://archive.nytimes.com/dealbook.nytimes.com/2012/02/01/tracking-facebooks-valuation/>

2. See: <https://www.dataguidance.com/opinion/eu-unpacking-eus-suite-new-era-digital-legislation>

3. See: <https://www.dataguidance.com/opinion/eu-unpacking-eus-suite-new-era-digital-legislation-2>

# The Ultimate Guide to US Privacy Laws

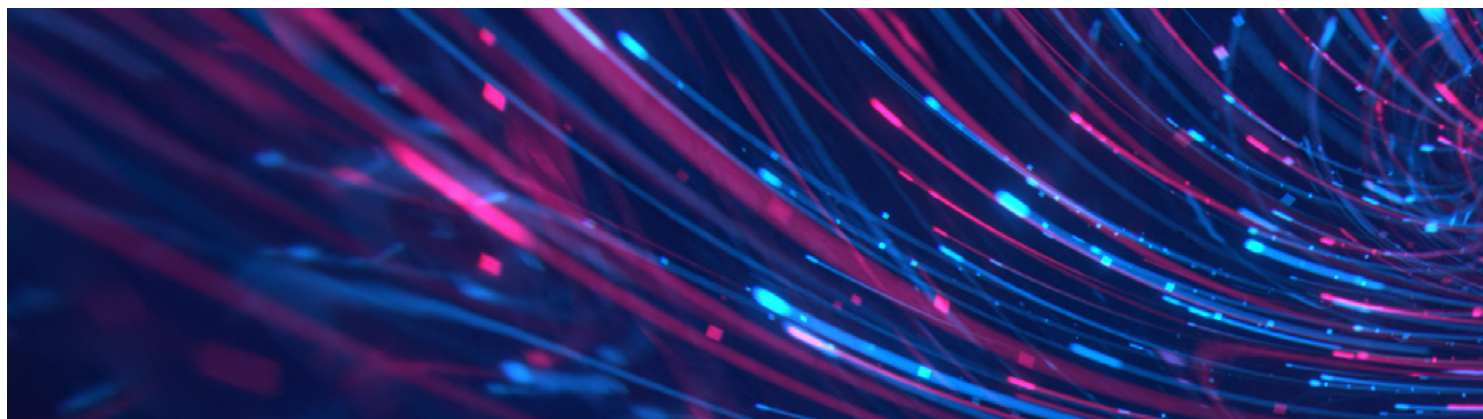
Get to know which states have joined the US privacy landscape, specific state law requirements, key timelines, comparisons, and more



## Download your copy

**OneTrust DataGuidance™**  
REGULATORY RESEARCH SOFTWARE





# Nigeria: Exploring AI recommender systems through the NDPA



**Akinkunmi Akinwunmi** Partner  
akin@paragonadvisors.com.ng  
Paragon Advisors

Many companies or data controllers deploy artificial intelligence (AI) to offer personalized suggestions to consumers or data subjects based on previous purchases, search history, or collected data and the consumers often follow those recommendations. For example, 80% of consumers for one video streaming service, stream based on AI recommendations and personalized content. The use of AI recommender systems raises concerns about whether data subjects are truly making their own decisions online, and the potential impact that AI recommendations could have on data privacy and protection.

The purpose of this article is to explore the effect of the Nigeria Data Protection Act 2023 (NDPA) on AI recommender systems. The article will examine if there are any applicable provisions within the NDPA and whether the NDPA effectively addresses privacy concerns that relate to AI recommender systems.

The article begins with a brief introduction to the AI recommender system and the associated privacy concerns. It then proceeds to analyze the NDPA to identify provisions that are relevant to AI recommendations.

## AI recommender system

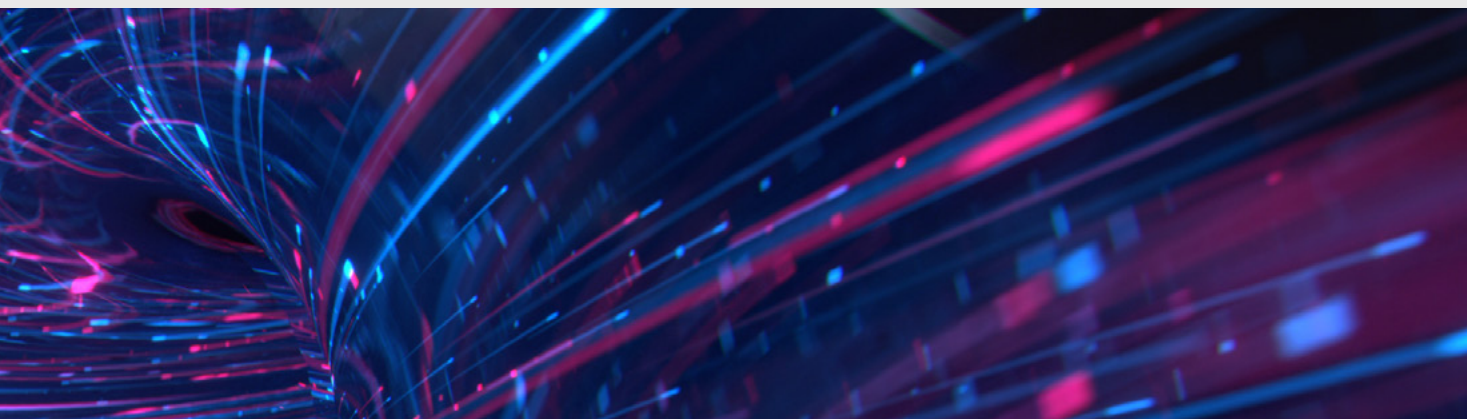
An AI recommender system is simply the use of AI to 'recommend products and services to the user of the product or services based on the preferences and choices of the user.' That is the use of AI to learn consumer behavior and use that knowledge to predict/ make suggestions regarding products or services that may be suited to the consumer<sup>1</sup>. For instance, when a consumer signs up for one video streaming service, the company collects biodata, financial data, geolocation data, and device data to provide customized and personalized viewing recommendations. The company also automatically collects and store information about the use of the video streaming, including information about interaction with its contents. Thus, each time a user selects a movie category, search title, or likes a movie, the service uses that data coupled with any other information to recommend movies.

AI recommendations improve the consumer experience on a platform, avoid information overload, and enable a consumer to make decisions easily without having to go through the entire catalogue of an online platform, thereby saving time and energy of the user

and ensuring consumer satisfaction<sup>2</sup>. The use of AI recommender systems by online platforms raises privacy concerns. Notably, AI recommendation systems do not only offer suggestions but interfere with consumers' decision-making process by subtly influencing and manipulating consumers' choices<sup>3</sup>. As a result, consumers inadvertently attribute movie, music, social, fashion, and political choices to their own preferences, unaware of the influence of AI on their choices<sup>4</sup>.

AI recommender systems rely on historic data of a data subject to reach its decision, thus, if the data collected is incorrect or biased, it could lead to a discriminatory recommendation that adversely differentiates, directly or indirectly and without justification<sup>5</sup>. For instance, a social media platform has been accused of discriminatory practices in its use of AI recommendations by showing job ads that relate to mechanics to male users while preschool jobs are shown mostly to female users. Biased output by an AI recommender system can cause physical or psychological harm to an individual or economic loss to a data subject<sup>6</sup>.

In order to be able to make recommendations to consumers, streaming platforms (for instance) may share consumers' personal data with third-parties or partners for various purposes, including advertising, analytics, data processing and



management, and hosting services. The privacy issue here is that these third parties may be unknown to the consumers, and the consumers may not have explicitly consented to any agreement or privacy policy with these third parties regarding their data. Consequently, consumers are unable to determine the full extent to which their data is being used by these third parties. Though the streaming platform might have stipulated the extent of use by the third party, consumers remain unaware and unable to object to the specific use of their data by these undisclosed third parties. Moreso, anonymized data shared may be reidentified by the third parties for their own use without the consent of the data subject and hereby posing a risk to the consumer. Thus, consumers lose control over their personal data.

The use of AI recommendations also poses a cybersecurity risk to the consumer. In the event of a cyberattack on the platform or third-party services, consumers are exposed to the risk of identity theft, cyberbullying, harassment, stalking, financial loss, and invasion of their privacy.

#### **AI recommender system and the NDPA**

Having examined the concerns surrounding AI recommendations, this article will now focus on the NDPA for any legislative solution.

Considering the widespread adoption of AI recommender systems across online stores, streaming services, and social media platforms, the expectation was that the NDPA would

have a specific part or section that addresses the privacy concerns above, but the NDPA does not explicitly cover AI recommender systems.

#### ***The use of AI recommender systems raises concerns about whether data subjects are truly making their own decisions online [...]***

Section 27 of the NDPA which requires data controllers to inform data subjects before collecting personal data was an opportunity to also mandate data controllers to (i) inform data subjects about the use of AI recommender system by data controllers; (ii) how the AI recommender system is deployed; (iii) the purpose of the AI recommender system, the information used by the AI recommender system; and (iv) limitations on its use. Rather, Section 27 of the NDPA focused on autonomous decision making which is clearly different from the AI recommender system. While the general provisions of the NDPA apply to AI recommender systems<sup>7</sup>, those provisions do not adequately address the privacy concerns above and are not tailored to address the challenges of AI recommender systems.

#### **Conclusion**

The NDPA represents a missed opportunity to enforce transparency and accountability among data controllers regarding their use of AI recommender systems. The NDPA

fails to establish liability measures for the utilization of AI and does not sufficiently prioritize data subjects' control over their data when AI is deployed. Additionally, the NDPA does not effectively address the potential biased outcomes that may arise from AI recommender systems.

As an interim measure, the Nigerian Data Protection Commission could leverage its statutory power under Section 62 of the NDPA to issue guidelines specifically addressing the use of AI recommender systems. These guidelines would serve as a stopgap until the National Assembly enacts a comprehensive law to regulate the use of AI recommender systems.

1. See: <https://doi.org/10.1007/s11257-023-09364-z>
2. See: <https://doi.org/10.1007/s40747-020-00212-w>
3. See: <https://doi.org/10.1080/1369118X.2016.1186713>
4. See: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3306006](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3306006)
5. See: <https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73> See also: <https://doi.org/10.1007/s10796-021-10156-2>
6. See: <https://doi.org/10.1007/s00146-020-00950-y>
7. See NDPA, Parts V and VI

## 5 MINUTES WITH...

# Goli Mahdavi



Goli is an attorney with the Bryan Cave Leighton Paisner Global Data Privacy & Security Group. Goli advises on the fullest range of data privacy compliance and strategy issues including cookies, data sharing, cyber incidents/personal data breaches, cross border transfers, and regulatory investigations across a range of sectors including technology, AR/VR, healthcare, and e-commerce. Goli is a founding member of the firm's Artificial Intelligence (AI) Task Force and her recent focus has been to help clients develop robust risk management policies and vendor management programs for their AI efforts.



### **Tell us a bit about your job role and how you have progressed in your career?**

As a senior member of Bryan Cave Leighton Paisner's Global Data Privacy and Security team I counsel a wide variety of companies across a host of industries on their compliance with domestic and international data privacy and protection regimes. In this role, I advise on data retention and minimization, Privacy by Design, cross-border transfer agreements, Privacy Impact Assessments and negotiating third-party agreements including digital marketing, software licensing, SaaS, and other commercial agreements.

I made my way to privacy after litigating for many years. I realized that what I enjoyed most about litigation (other than the thrill of securing a favorable outcome for my client) were the opportunities that I had to work with companies to understand their business operations, and make changes and improvements to address compliance issues. Data privacy has given me the opportunity to provide strategic counselling to our clients, help them bring new products to market, and work collaboratively across multiple business lines to implement new strategies.

More recently I worked to form the firm's Artificial Intelligence (AI) Task Force to help our clients leverage

the power of AI while managing the potentially significant reputational, regulatory, security, and legal risks.

### **What alternative job would you have if you had not gone into law?**

There was a period of time in my undergraduate days when I very seriously considered majoring in interior architecture. While I ultimately made the right career choice, there is a residential design itch that does need to be scratched from time to time. My family often sees me holding a tape measure and staring at a wall, wondering if it's load bearing.

### **What do you love about your job, and what do you find challenging?**

I love being at the intersection of the law, business operations, and technology. One of my legal mentors believed that lawyers must reinvent themselves every few years and I love that because the technology and regulations keep progressing - that process of reinvention is effectively built into my practice. That constant organic innovation is also the main challenge of my practice because there is always some new development to consider.

### **Where is your favorite place on earth?**

Sea Ranch, California. A beautiful town that stretches across 10 miles of the Northern California coastline. It was built up in the 1960s by architects dedicated to designing homes that are harmonious with the landscape. Both the natural and man-made environments are stunningly beautiful and rugged. It is the perfect escape from urban life.

### **Who would play you in a film about your life?**

While I'm very happy with my personal

and professional life this film would be a box office flop, so I hope no one is cast in the role for their sake!

### **What is your favorite book?**

The Jungle by Upton Sinclair has always stayed with me. An early example of the power of investigative journalism, and the power of one person to drive systemic change.

### **What is some advice you would give to others starting off in your industry?**

Let your intellectual curiosity lead you. Most working professionals dedicate the majority of their waking hours to their careers, and because lawyers are in the business of serving their clients, there are very few boundaries between work and life. If we are so lucky to find ourselves actually interested in the subject matter that we are advising on – as cliché as it may sound – it feels a lot less like work.

### **Who is your inspiration?**

It wasn't until I had a family of my own that I fully appreciated what an incredible feat it was for my parents to immigrate to the US with a young child in tow and no social or financial safety net to speak of. I am so inspired by their resilience and determination, and it helps me put things in perspective and push through when things get tough.



# Interested in Becoming a OneTrust DataGuidance Contributor?

Partner with the world's most widely used technology platform to manage privacy, security, and data governance and help organizations be more trusted. Law firms around the world partner with OneTrust DataGuidance because we are committed to and invested in their success.



Send Your Submissions to: [contribute@onetrust.com](mailto:contribute@onetrust.com)

**OneTrust DataGuidance™**  
REGULATORY RESEARCH SOFTWARE

Data Protection Leader is published bi-monthly by OneTrust Technology Limited, Dixon House, 1 Lloyd's Avenue, EC3N 3DS, London, United Kingdom

Website: [www.dataguidance.com](http://www.dataguidance.com)

Email: [DPL@onetrust.com](mailto:DPL@onetrust.com)