DATA PROTECTION LEADER

Volume 5, Issue 1
January 2023
dataguidance.com

Ideas shaping privacy, published by OneTrust DataGuidance™

TACKLING THE AI REGULATORY CHALLENGE

EU AI ACT

Exploring the latest developments and practical implications of the AI Act

COUNTRY PROFILE

A look at the current and upcoming laws in the US and how organisations can navigate them

INDIA'S NEW BILL

Outlining the changes to the Digital Personal Data Protection Bill

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

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.

Alex Sharpe, Sharpe Management Consulting LLC
Mr. Sharpe is a long-time (+30 years) Cybersecurity, Governance, and Digital Transformation expert with real-world operational experience. Mr. Sharpe has run business units and has influenced national policy. He has spent much of his career helping corporations and government agencies create value while mitigating cyber risk. This provides him a pragmatic understanding of the delicate balance between Business realities, Cybersecurity, and Operational Effectiveness. He began his career at NSA moving into the Management Consulting ranks building practices at Booz Allen and KPMG. He subsequently co-founded two firms with successful exits including the Hackett Group (NASDAQ HCKT). He has participated in over 20 M&A transactions. He has delivered to clients in over 20 countries on 6 continents.

Dr. Carlo Piltz, Piltz Legal
Carlo accompanies and advises national and international clients in questions of data protection, IT security, and IT law. Carlo supports compliance and legal departments as well as internal data protection officers in day-to-day business as well as in complex cases and contract negotiations. Carlo also works as an external data protection officer. Carlo's passion is also administrative law and he has successfully completed the theoretical training to become a specialist lawyer for administrative law. Carlo was invited to the respective parliaments as an expert for both the new version of the Federal Data Protection Act and the Berlin State Data Protection Act.

Monika Tomczak-Gorlikowska, Prosus Group
Monika Gorlikowska is the Chief Privacy Officer of Prosus N.V. - a global consumer internet group and one of the largest technology investors in the world. She is based in Amsterdam and previously was the Senior Data Privacy Legal Counsel with Shell International Limited in London. She has practice data privacy law for more than 20 years. Monika is a licensed attorney (adwokat) and in the past was in private practice, amongst others with the offices of Miller, Canfield in Poland. In addition to the law studies, she has also received a Master of European Law degree (LLM cum laude) from the Law Department of the College of Europe in Brugge (Belgium). Monika also served as Co-Chair of the Steering Committee of the Forum on International Privacy Law and currently a member of the Steering Committee.

Spiros Tassis, Tassis & Associates Law Office
Spiros has been an IT Law, Data Protection, and Privacy lawyer since 1999. Spiros is a member of the Bar of Athens (Supreme Court), chair of the Hellenic Association of Data Protection and Privacy (HADPP), BoD of the EFDPO, founder and former co-chair of the #IAPP Greek Knowledge Chapter, Associate of the Department of Applied Informatics, University of Macedonia, and a member of the AI in Justice committee. In 2010, Spiros established the Tassis & Associates Firm, which is now a leading TMT and Privacy law firm in Greece running data management and compliance projects for major entities and organisations of the private and public sector.

Stephen Mathias, Kochhar & Co.
Stephen Mathias is the head of the Bangalore office of the Firm and co-chair of the Firm's Technology Law Practice. Stephen is a graduate of the National Law School of India University where he did an Honours degree in Arts and Law. He is also a British Chevening Scholar and has done a diploma in European and English Law at the College of Law York and worked briefly at a leading law firm in London. He is also a solicitor on the rolls of the Law Society of England and Wales. Stephen does substantial data privacy work, mostly assisting multinationals in understanding data privacy law implications in the way they deal with personal data. He has also led teams investigating and taking enforcement actions in cases of data theft.

Image production credits
Cover / page 4 image: Alena Butusava / Essentials collection / istockphoto.com
Page 6-7 image: shulz / Signature collection / istockphoto.com
Page 10-11 image: skodonnell / Signature collection / istockphoto.com
Page 16-17 image: Instants / Signature collection / istockphoto.com
Page 20-21 image: inkoly / Essentials collection / istockphoto.com
Page 24-25 image: BrAt_PiKaChU / Essentials collection / istockphoto.com
Page 26 image: tigristiara / 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**

Email **DPL@onetrust.com**

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

Editor **Eduardo Ustaran**
eduardo.ustaran@hoganlovells.com

Managing Editor **Alexis Kateifides**
akateifides@onetrust.com

Editorial Lead **Victoria Prescott**
vprescott@onetrust.com

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

CONTENTS

AI regulation is being drafted with a heightened degree of urgency and a global patchwork of rules and laws governing AI are already making their way into the statutory books

Editorial: Tackling the AI regulatory challenge

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

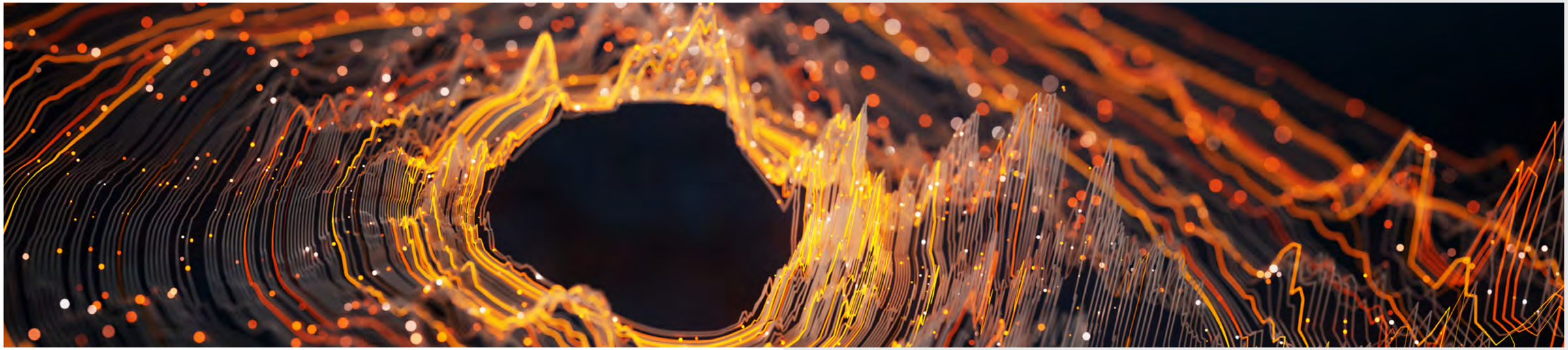
ChatGPT has taken the world by storm by simply making artificial intelligence and its awesome power available to all. AI is certainly not new, but its daily presence is more palpable than ever before. To put it differently, if there was ever any doubt, AI is here to stay and possibly to change our lives. But since history has taught us to approach radical technological changes with caution and scepticism, policy makers and regulators around the world are rushing to provide a dose of wariness aimed at ensuring that the development and implementation of AI addresses its own risks. AI regulation is being drafted with a heightened degree of urgency and a global patchwork of rules and laws governing AI are already making their way into the statutory books. This raises important policy, professional, and compliance questions.

From a public policy perspective, the obvious challenge is how to regulate AI in a way that maximises its economic and societal promises and benefits, whilst eliminating the potential for harm, unfairness, and inequality. One can debate how detailed or light touch AI regulation should be, but there seems to be a universal consensus around the fact that whatever framework is devised to regulate AI, it should be risk-based and, ideally, future-proof. In practice, this means that for AI regulation to succeed in achieving its objectives, it must be able to adapt to all types of situations and therefore rely on principles rather than prescriptive rules. It is also essential to be aware of the global dimension of AI and to approach this challenge in the most internationally collaborative way. As various legislative initiatives in this space take place around the world, global consistency must become a crucial reference point.

The emerging AI regulation is also creating a professional conundrum. Who will be best equipped to help navigate the strategic and operational challenges presented by the new legal framework given its novelty and multi-disciplinary nature? The work opportunities for a new generation of AI regulatory specialists are obvious but who is best placed to take a leading role in this area today? Looking at the issues at stake - fair data collection and usage, automated decision-making of life changing consequences, risk management responsibilities - it seems clear that this is familiar territory for privacy and data protection professionals. So, in the same way that our collective knowledge and judgment in relation to privacy and cybersecurity matters is necessary to reap the benefits of data while addressing the risks of misuse, those skills are likely to be put to the test in the context of AI. It is also not a coincidence that the new European AI regulatory framework is borrowing concepts and obligations from laws like the GDPR, as the methodology for dealing with the potential risks of AI is largely transferable.

Speaking of the emergent EU AI Act, which in terms of compliance obligations, is at least as wide-ranging and ambitious as the GDPR, the time to pay attention to what is coming and what to do about it is now. Any organisation involved in the development or potential use of AI technology today will be wise to familiarise itself with the diverse but complementary requirements that form part of this developing framework. At the very least, organisations should be seeking to undertake an AI regulation impact assessment to determine the extent to which their systems are likely to be subject to the law, and if so, decide how best to prepare for it. As different AI laws make their appearance in different jurisdictions, devising and implementing a global AI regulation compliance program covering issues such as data governance, transparency documentation, and human oversight strategies will resemble a search for the holy grail.

AI may be a difficult issue to pin down - partly because of its underlying technological complexity, partly because its development is taking place in front of our eyes at breath-taking speed, and partly because the implications of its widespread adoption will be crucial for the future of humanity - but what is clear is that it is attracting huge regulatory attention at a global scale. That is not necessarily a bad thing but for AI regulation to achieve its goals, we must be prepared to move fast, be creative, and think globally whilst being as pragmatic as possible.



EU: AI Act - state of affairs and a brief analysis of the latest developments

Dr. Carlo Piltz Partner
carlo.piltz@piltz.legal
Piltz Legal

Background: European Commission's proposal for the AI Act

In April 2021, the European Commission published its proposal[1] for the AI Act. Being a part of the so-called European AI Strategy[2], which aims at making the EU a world-class hub for AI and ensuring that AI is human-centric and trustworthy, the AI Act lays down some basic rules in relation to AI systems, their development, and their implementation. With the AI Act, the Commission wants to ensure that AI systems on the EU market are safe and respect existing fundamental rights law and to enhance governance and effective enforcement of existing law and safety requirements applicable to AI systems. Furthermore, through a harmonised approach, it aims to ensure legal certainty in order to facilitate investment and innovation in AI. Among other proclaimed objectives of the act is facilitating the development of a single market for lawful, safe, and trustworthy AI applications and to prevent market fragmentation.

Even though the text of the proposed AI Act is far from being final, most of the basic elements and mechanisms of it are unlikely to change fundamentally at this point. The cornerstone of the AI Act is a risk-based approach, which ensures that the regulation does not indiscriminately impose significant regulatory burdens for all AI systems. The regulation differentiates between three levels of risk to the health and safety or fundamental rights of natural persons.

The first category includes a list of AI practices which are considered to bear unacceptable risks, in particular systems which are designed to manipulate people through various techniques or to exploit vulnerabilities of specific groups, such as children or persons with disabilities, are prohibited.

The second proposed category are the high-risk AI systems. In Annex III of the AI Act, the Commission provides a list of areas in which the AI systems are to be considered high-risk. However, the list is a rather general non-exhaustive enumeration. Apart from the Annex III, a broad spectrum of AI systems which are intended to be used as safety components is also considered high-risk (Art. 6 (1) AI Act). The proposed regulation contains multiple mandatory requirements in relation to such systems. Establishing and implementing risk management and data governance systems (Articles 9 and 10 of the AI Act), and drawing up technical documentation and record-keeping (Artices 11 and 12 of the AI Act) are essential when developing or using a high-risk AI. Further obligations include transparency towards the users (Article 13 of the AI Act) and interface tools allowing for human oversight (Article 14 of the AI Act), as well as appropriate levels of accuracy, robustness, and cybersecurity. These minimal requirements are complemented by a set of obligation of providers, users, and other parties (including but not limited to importers, distributors, and authorised representatives) in relation to documentation, quality management, and notifications to the competent authorities (Title III, Chapter 3 of the AI Act).

Systems which are not considered high risk are for the most part exempted from the regulatory obligations and only need to be transparent towards their users. For example, if an AI system is used to generate or manipulate video content (so-called 'deep fakes') it should disclose that the content is generated through automated means, e.g., by providing a description or a watermark. If the AI nature of the system is obvious from the circumstances and the context of its use, even that is not required.

Apart from the obligations, the AI Act contains several measures aiming to support the innovation in the AI field. Main instrument of the regulation are the AI regulatory sandboxes (Article 53 of the AI Act), which should provide a controlled environment allowing for developing, testing, and validating innovative AI systems before real-world-tests. While remaining liable for any harm inflicted as a result of the experimentations, the AI developers can significantly lower the risks when testing their products in the sandbox environment.

Other provisions of the proposed act include establishing the European Artificial Intelligence Board (Article 56 of the AI Act) and providing a legal framework for control mechanisms such as post-market monitoring (Article 61 of the AI Act). Naturally, the AI Act follows the turnover-based penalties concept (up to 6% total worldwide annual turnover or a fine up to €30 million, whichever higher), which can be found in the majority of current EU acts and regulation proposals.

Changes in the Council's common position

On 6 December 2022, the Council of the European Union adopted its common position[3] on the AI Act. Even though it does not change the structure and the general approach of the Commission's proposal, there are certain adjustments which are immensely important.

One major change to the regulation concerns the definition of an AI system. In order to address a general concern of the EU Member States that the new regulation will apply also to the 'classical' software systems, the Council's document provides the following definition:

'a system that is designed to operate with elements of autonomy and that, based on machine and/or human-provided data and inputs, infers how to achieve a given set of objectives using machine learning and/or logic- and knowledge based approaches, and produces system-generated outputs such as content (generative AI systems), predictions, recommendations or decisions, influencing the environments with which the AI system interacts'.

This approach narrows down the definition from the Commission's proposal significantly and introduces additional criteria: elements of autonomy, machine learning, and logic- and knowledge-based approaches. As intended, this new definition excludes the classical software and systems based on merely statistical approaches from the regulation scope. Interestingly, this definition is closer to the one in 2018 Communication on Artificial Intelligence for Europe[4], a paper laying out the EU's approach to the AI, rather than the 2021 Commission proposal for the AI Act. Due to the striking similarities, it can also be speculated that the new definition was inspired by the OECD interpretation of the term 'AI system'[5].

As it seems, the consensus on the definition of an AI system will be difficult to achieve in the upcoming trilogues, as the Commission, the Council, the Committee of Regions[6], and the Economic and Social Committee[7] all provide different definitions with the European Parliament's position still pending. It is especially concerning as it could result in a watered-down definition aiming to compile different approaches, which would create uncertainty as to the scope of the AI Act.

The changes by the Council are not limited to the AI definition. The proposal extends the list of unacceptable AI practices and prohibits AI-based social scoring also for the private actors. Furthermore, the Council includes exploiting economically and socially vulnerable groups of persons to the list of prohibitions, which could potentially have effect on credit score systems. The proposal also limits the objectives where using remote biometrical identification systems by law enforcement authorities is allowed.

Classification rules and requirements for high-risk AI systems have also been

specified by the Council. This includes not only clarifications concerning technical documentation for compliance demonstration, but also the relationship between responsibilities under the AI Act and other legislation. Furthermore, the Council's common position enhances transparency and provides an exclusion for national security, defense, and military purposes.

In line with a general more business-friendly approach of the Council, some changes to the provisions related to developing and testing innovative AI systems have been made. For example, the regulatory sandboxes should allow for testing of the innovative systems in real world conditions and under specific safeguards, unsupervised real-world testing must be made possible.

Finally, the new proposal introduces additional provisions tailored to fit the general-purpose AI systems. If a system can be used for many different purposes, there may be circumstances where such technology, without being a high-risk one by itself, gets integrated into another system and becomes high risk. Regulation of the general-purpose AI is essentially made dependent on various implementing acts, specifying how the AI Act provisions should apply to such systems.

Overall, the Council's text is more specific than the initial proposal by the European Commission and aims to provide more legal certainty while remaining flexible to include possible future AI systems.

Practical implications of the AI Act and outlook

The AI Act applies both to providers and users of AI systems. To users, the provisions only apply in professional context and personal activity is explicitly excluded from the scope. 'Provider', in essence, means the developer of an AI system or a distributor who places the system on the market under own name or trademark. As for the territorial scope, the providers must either place their AI systems on the European Union market or the output of the AI systems must be used in the EU. The provisions only apply to those users who are located within the EU. In short, if an AI system is either present on the EU market, is being used in the EU, or its output is used for the EU market, the users and providers of the system are subject to the proposed AI Act.

A more complicated question is what systems and products are affected, as it depends on the AI definition. As of now, it is hard to say which definition will prevail in the final document, but it is certain that AI systems in a wide variety of areas will be subject to new obligations. Apart from the systems explicitly mentioned (and prohibited) in the AI Act, such as social scoring, based on the current proposals, some systems can already be identified and sorted by risk levels. For example, intelligent management systems for water, power, and heating supply; credit decisions and financial documents processing software or advanced CV parsing systems will almost certainly fall into the high-risk category. Chatbots, deepfakes, and intelligent spam-filters on the other hand can be considered low risk. In general, any system utilising machine learning (including deep learning) will certainly be considered an AI system under any of the proposed definitions.

In the last few months, substantial legislative progress was made with regard to the AI Act. Apart from the Council's position, a proposal for the AI Liability Directive[8] has been published, which aims to lay down uniform rules for certain aspects of civil liability for damages caused by AI involvement and complements the provisions of the AI Act. As soon as the European Parliament's position is adopted, the trilogue negotiations will begin. Given the fact that over 3,000 amendments were being considered as of April 2022 and major differences in such fundamental aspects as the AI system definition, there is little hope for a swift adoption. No exact prognosis is possible, but it is unlikely that the provisions will be applicable before 2024.

Even though there are many steps in the legislative process yet to make, there are already some things that the companies can do. AI systems which are already in use should be identified as such (as it may not always obvious for those who do not deal with technical aspects), and an initial rough assessment should be carried out in order to forecast into which risk category the system is likely to fall. Especially if the assessment shows high risk, additional costs for compliance should be kept in mind. It is advisable to start preparing for the upcoming act to the extent possible already now in order to ensure that the new regulations do not come unexpected.

1. See: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206
2. See: https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence
3. See: https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf
4. See: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0237&from=EN
5. See: https://oecd.ai/en/ai-principles
6. See: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021AR2682
7. See: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021AE2482
8. See: https://commission.europa.eu/system/files/2022-09/1_1_197605_prop_dir_ai_en.pdf

Country Profile: USA

Navigating the concophony of privacy laws in and out of the US

The myriad of Privacy Laws in the US, combined with the various specialty laws, regulations, and international laws, can be confusing and sometimes in conflict. This article will map out the landscape, look into the future, and share street knowledge on how to navigate the landscape.

Alex Sharpe Principal
alex@sharpellc.com
Sharpe Management Consulting LLC

Introduction

Most of what is written about privacy is by lawyers for lawyers or individuals. This article is written for business leaders looking to make informed decisions and practitioners looking to implement with limited resources without undue risk.

Under the covers, privacy is about promoting commerce by establishing guard rails, enforcement, and transparency to foster digital trust. In essence, privacy is a data governance and a compliance problem.

Why is privacy so complicated? In the US, privacy laws are driven by the states rather than at a national level.

Globally, almost 130 countries have privacy laws. That would be more if it were not for the creation of the General Data Protection Regulation (GDPR) – effectively a single privacy law covering 27 countries.

Privacy is tied to data protection and breach laws. For example, California probably has the most recognised privacy law in the US. It also has north of 25 data protection and breach laws. Quite often, when there is an incident, the organisation must deal with privacy and data protection and breach notification laws together.

Fifty-four jurisdictions in the US have breach notification laws. Why 54 when there are only have 50 states? Simple, Washington DC, Guam, Puerto Rico, and the U.S. Virgin Islands have breach notification laws. The Tribal Nations are separate and sovereign jurisdictions that can make their own. This was determined through a series of cases known as the Marshall Trilogy[1]. In addition, we need to look at federal laws, sectoral regulations (e.g., finance), and international laws such as the GDPR.

EU-US Data Privacy Framework and OECD Declaration

It is all too easy to lose sight of the purpose underlying privacy. Privacy promotes commerce by fostering digital trust with guardrails, transparency, and enforcement. We not only need to do so within states and between states but also internationally.

In July 2020, the Court of Justice of the European Union (CJEU) found that US domestic laws do not adequately protect personal data in what has become known as the Schrems II decision. The decision also concluded that US federal laws do not provide adequate protection against the use by US public authorities of data transferred from the EU.

Schrems II effectively struck down the EU-U.S. Privacy Shield as a valid data transfer mechanism under EU law. Schrems II severely undermined the transatlantic data flows – placing the $7.1 trillion economic relationship between the US and the EU in jeopardy. US and EU companies, large and small, across all sectors of the economy depend upon cross-border data flows to participate in the digital economy and expand economic opportunities.

The EU-US Data Privacy Framework (DPF) was negotiated to replace the former EU-U.S. Privacy Shield Framework.

To restore trust and stability to the U.S.–EU economy, on 7 October 2022, the Biden Administration signed the Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities (the EO) - the latest US action to implement the EU-US DPF and reiterates our shared values.

Why 'Enhancing Safeguards for United States Signals Intelligence Activities?' It is relatively simple; one criticism of the Schrems II decision is that the current signals intelligence collection does not address all GDPR principles directly. When it comes to the protection of personal data, current laws do not limit to what is 'strictly necessary' and do not 'lay down clear and precise rules' that 'impose minimum safeguards'. The EO basically:

- bolsters an already rigorous array of safeguards to ensure privacy and civil liberties are aligned with GDPR principles;
- creates redress mechanisms for people who believe their data was collected in a way that violates US law; and
- charges the Privacy and Civil Liberties Oversight Board (PCLOB) to review intelligence community policies and procedures to ensure that they are consistent with the EO and to conduct an annual review of the redress process.

American Data Privacy and Protection Act

It has been about 12 years since Congress took a run at creating a national privacy law. On 20 July 2022, the U.S. House of Representatives passed the American Data Privacy and Protection Act (ADPPA). To become a law, the ADPPA still needs to be passed by the Senate and signed by the President. Whether that will happen in 2023 is yet to be seen. At the very least, the ADPPA is creating a conversation about harmonising the various state actions, not recreating the wheel. The ADPPA is mapping out the core principles seen in many of the state's privacy laws.

Why is it so hard to create a federal privacy law? There seem to be two generally accepted reasons.

First, many states, like California, see a Federal law as weaker than what they already have, undermining their actions.

Second, some argue that the US Congress does not have the authority. The word 'privacy' does not appear in the US Constitution and is, therefore, a right of the states. There is precedent for the US Congress' authority when it comes to legislating government actions regarding the right of citizens, but that is limited to the action by government bodies like law enforcement. There is no apparent authority for the Federal Government to legislate the activities of private entities and consumers when it comes to privacy.

What makes the ADPPA different? Instead of a general requirement that companies consider privacy in the design of their processes, the ADPPA only allows companies to collect and use user data if necessary for one of 17 permitted purposes. Uses outside of that are expressly prohibited.

Unlike some of the state laws, the ADPPA is straightforward regarding applicability. The ADPPA would govern how companies across different industries treat consumer data. Most entities, including nonprofits, are subject to the ADPPA.

The ADPPA is also straightforward on what data '...identifies or is linked or reasonably linkable' to an individual.

For possibly the first time, the ADPPA also treats a broader definition of 'data' and recognises that all private information is not equal – some is more important than others. For example, genomic data, such as DNA, is considered private.

Enforcement would be provided by the Federal Trade Commission (FTC), which implies authority over transactions between states.

How does each of the five states compare?

Let us walk through how each of the five state privacy laws are alike and how they are different. Privacy laws can be viewed from many different lenses.

We will focus on what is germane to decision-makers and practitioners.

As of 1 January 2023, five US states have specific privacy laws:

- California (CA);
- Virginia (VA);
- Colorado (CO);
- Utah (UT); and
- Connecticut (CT).

These five will undoubtedly establish the foundation for all future privacy laws in the US. They are more alike than different. In fact, in some areas, they share language. In general, CA is the most restrictive and casts the widest net. All build upon existing federal laws and secular regulations, which should provide some reduction in the regulatory burden and the cost of compliance.

When it comes to third parties, the number one thing to remember is that you can delegate responsibility but cannot delegate accountability.

The Gramm-Leach-Bliley Act (GLBA) already requires financial institutions to protect consumers' financial information.

The Health Insurance Portability and Accountability Act (HIPAA) already requires covered entities to prevent sensitive patient health information from being handled contrary to the patient's instructions and from not being disclosed outside of certain procedures.

The Children's Online Privacy Protection Act (COPPA) provides guidelines for protecting the privacy of children under 13.

The US Privacy Act of 1974 empowers individuals to request records about themselves in possession of government agencies.

All five states provide consumers with the:

- right to know what personal information is collected, how it is used, and how it is shared;
- right to delete personal information with some exceptions;
- right to opt out of the sale of their personal information;
- right to non-discrimination for exercising their rights;
- right to be properly notified; and
- right to have privacy practices explained clearly.

Applicability

State privacy laws apply to businesses and data brokers operating in a state or selling to citizens of the state. All agree that a business is a for-profit entity. The applicability comes down to three factors. Each state has its own threshold(s).

- annual revenue;
- the number of consumers the entity receives, buys, or sells the personal information; and
- the percentage of revenue derived from consumer personal information.

Except for CA, each state provides a list of bodies to which the privacy laws do not apply.

CO does not apply to air carriers and certain national securities associations.

CT provides an extensive list of bodies its privacy law does not apply, including state bodies, nonprofit organisations, institutions of higher education, certain national securities associations, certain financial institutions regulated by federal law, and covered entities and businesses regulated by federal law.

UT does not apply to governmental entities or third parties under contract to a governmental entity when acting on behalf of the government. Like other states, UT does not apply to institutions of higher education, nonprofits, and covered entities regulated by relevant federal laws. UT is the only state that specifically states it does not apply to tribal nations.

VA does not apply to VA government affiliates and financial institutions, covered entities regulated by relevant federal laws, nonprofit organisations, and higher education institutions.

Penalties/enforcement

Of the five, only CA has a dedicated authority established. The rest rely on the State Attorney General.

The role is similar across the five states, with some differences in cure periods. CA cure period is discretionary. UT and VA provide for 30 days, while CO and CT provide a 60-day cure.

Each of the five laws contains monetary penalties. These penalties are in addition to what may be leveled for related acts or by other bodies. The basis for penalties, amounts, and how they are regarded are nuanced and probably best analysed using scenarios.
CO and CT do not expressly provide for set penalties; instead, they treat a violation as an unfair or deceptive trade practice. Setting limits of $20,000 and $5,000, respectively, per incident.

CA, UT, and VA provide for penalty amounts within their laws. CA's penalties range from $2,500 per violation to $7,500 for each intentional violation. UT and VA specify a penalty of no more than $7,500 per violation.

It is common practice to perform a cost-benefit analysis when determining investments. At first blush, these numbers appear to be deceptively small and could lead to an underinvestment in controls and privacy programs. Keep in mind that these numbers can snowball depending on the nature of the incident and are in addition to what may be levied by other jurisdictions and regulatory bodies.

We also cannot lose sight that this is consumer data. The most significant long-term loss may be the reputational damage and loss of digital trust.

Definition of personal information

All five states cover traditional categories like health status, ethnicity, religious beliefs, sexual orientation, citizenship, and the like. CA has the most extensive list, but nothing surprising. All but CO regard geolocation as sensitive personal information. Happily, all five states provide for the protection of genetic and biometric data. The value and the need to protect genetic and biometric data has received increasingly growing attention over the past few years. In this area, the state privacy laws demonstrate a forward-looking approach to lawmaking.

Information regarding children has long received special attention in the privacy space. This attention is reflected in the state privacy laws as well. CA, VA, and CO have specific callouts for children, while CT and UT are silent.

Territory

The privacy laws of all five states regard the residents of that state and apply to any organisation within the state or organisations targeting residents of the state. Only CA calls out residents out of the state. The remaining four are silent on the subject.

Private right of action

Whether to provide personal remedies or not is one of the most highly debated topics in the community. CA is the only one of the five states that provides for an individual's right of action due to data breaches. Other than that, the five states are wholly aligned in not providing for individuals' private right of action for any violations.

CO explicitly states it does not authorize a private right of action. The remaining states take it one step further, noting that nothing in the privacy law can be construed as providing the basis for a private right of action.

Data transfers

None of the five laws address cross-border transfers directly. They leave that to other laws and regulations. Within the laws, they deal with transfers to third parties.

CA, CO, and CT address the obligations related to the transfer and sharing of information with third parties. UT outlines what does not constitute the sale of personal data and generally notes that consumer authorisation is required for any disclosure. VA only outlines what does not constitute the sale of personal data by addressing certain disclosures and providing provisions like what we see in CT's privacy law.

Breaches

None of the states specifically address breaches within the privacy laws. Instead, they rely on other state, federal, and international statutes. The slight exception is CA, which deals with breaches to the extent that it provides relief for consumers whose personal information was compromised during a breach.

In practice, dealing with breaches and breach notifications is an area that requires attention long before an incident occurs. In effect, notifications are required within 72 hours of discovery. Who must be notified, what they require, and ongoing reporting varies. For example, CA has a single privacy law but at least 25 laws with reporting requirements.

This reporting is in addition to what is required by other states, regulators, and internationally. The burden placed on a global publicly traded company can be significant. Incidents are stressful enough. The last thing you want is the added confusion from all this reporting and any fallout from non-compliance. The best tact is to sort this out long before an incident occurs – dig your well before you are thirsty.

Privacy notice

All five states require a clear, conspicuous, and material privacy notice.

Data Protection Assessment

CT, VA, and CO each require some level of a Data Protection Assessment (DPA), especially for data at a higher risk to the consumer. UT is silent on the subject. CA is subject to rule making.

On a practical note, you will need to perform a data mapping exercise to ensure the proper level of protection at a reasonable cost. More than likely, your organisation has already done some level of a DPA as part of an overall Business Impact Assessment (BIA) or Information Systems Security (INFOSEC) exercise. In a perfect world, you will have performed a Privacy Impact Assessment (PIA).

Opt-in/opt-out

The option to opt-in or opt-out has become accepted practice in the digital world and will most likely only become more prevalent as the breadth and depth of services continue to grow (e.g., Metaverse). Four of the five states (not UT) require clear and conspicuous opt-in functions that the consumer can change at any time. UT seems to prefer an opt-out strategy with two exceptions. First, parental consent is required BEFORE processing if it regards a child. Second, UT also talks about any means specified by the controller. What that means in practice should become apparent over time.

States with privacy Laws on the Docket for 2023

As discussed, within the US, any jurisdiction – State, possession, territory – can write a data protection law. The same is true for privacy laws. Regulators and sectors can as well.

Whilst five of the 50-plus jurisdictions have privacy laws, four states have proposed legislation in committee that will most likely become law in 2023 (Michigan, Ohio, Pennsylvania, New Jersey). Fortunately, these proposed draft legislations are consistent with what we see from the five existing laws. Of the remaining states, 23 have inactive bills in various stages.

What is an organisation to do?

Many firms are willing to help your organisation interpret the various laws and regulations. Let's discuss how to get it done based on years of street knowledge.

Net-net, privacy is about data governance and compliance. Two well know disciplines across many sectors. As you have seen, while there are many privacy and privacy-related laws and regulations, they are more alike than different.

We also cannot lose sight that this is consumer data. The most significant long-term loss may be the reputational damage and loss of digital trust.

The first step is to know your data and your business model. Perform a PIA. A PIA is very much like a BIA but with a privacy focus. The objective of a PIA is to determine if collected personal information data is necessary and relevant. Determine what you collect, what you retain, and where it is located. Be sure to look at where the data is not only stored but also where it is processed and where it is transmitted.

Know where your data resides. Confine the data to the greatest extent practical - bits don't know borders but the law and consumers do.

Hold it only as long as necessary, and do not collect what you do not need. Privacy information generally does require the same level of protection as more sensitive information. Look where it makes sense to use techniques like tokenisation and anonymisation to reduce your exposure at a lower cost.

In my experience, third parties are your weakest link. Do your due diligence and leverage contractual agreements and Service Level Agreements (SLAs). Be sure they address:

- data ownership;
- confidentiality;
- cyber incident liability and reporting;
- compliance with applicable laws; and
- geographic location(s).

When it comes to third parties, the number one thing to remember is that you can delegate responsibility but cannot delegate accountability.

Incidents rarely stand alone. Privacy incidents often come as part of a cyber incident or a data breach. As part of your incident response planning, take a hard look at reporting - what needs to be reported to whom and when. The best way to do this is through scenarios.

Lastly, create a privacy aware culture. Include privacy in all of your training and awareness programs.

1. See: https://www.americanbar.org/groups/crsj/publications/human_rights_magazine_home/2014_vol_40/vol--40--no--1--tribal-sovereignty/short_history_of_indian_law/

INFOGRAPHIC

California Privacy Rights Act Overview

Overview

The CPRA passed in 2020 and became effective on January 1, 2023. The CPRA amends and extends sections of the CCPA.

Timeline

JUNE 28 2018
CCPA signed into law

JAN. 1 2020
CCPA goes into effect

NOV. 4 2020
CPRA is passed

JULY 1 2020
CCPA enforcement begins

JAN. 1 2023
CPRA goes into effect – employee and B2B exemptions expire

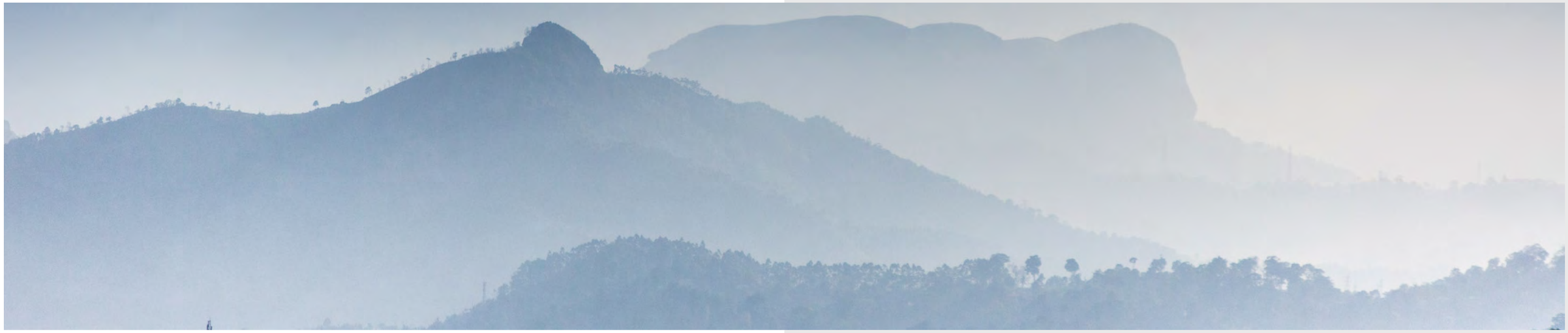
JULY 1 2023
CPRA enforcement begins

Scope of application

THE CPRA APPLIES TO

For-profit businesses that collect personal information from California residents

AND
Have gross annual revenue of over $25 million
OR
Buy, sell, or share personal information of 100k+ California residents or households
OR
Derive 50%+ of annual revenues from selling or sharing personal information of Californians



India: A review of the new Digital Personal Data Protection Bill

In mid-November 2022, the Ministry of Electronics and Information Technology ('MeitY') released the fourth draft of India's proposed Digital Data Protection Bill, 2022 ('the Bill'). It has been more than four years since the first draft was released in 2018. At first glance, the Bill seems quite unusual. It is much simpler and shorter than the previous versions and it also differs substantially from the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') style legislations that are commonplace today. Gone are the detailed notice requirements; there is no reference to Privacy by Design or data portability and no separate treatment of sensitive personal data. There are also no provisions on data localisation. In this article, Stephen Mathias, Senior Partner from Kochhar & Co., analyses some of the key concepts in the Bill.

Deemed consent

The Bill provides for consent as the key ground for collection and processing of personal information ('PI'). In addition, there are two sets of grounds under 'deemed consent', both of which are tied to necessity. One set refers to certain grounds but qualify that those grounds must be in the 'public interest'. This covers grounds such as the prevention and detection of fraud, mergers and acquisitions, network and information security, credit scoring, and recovery of debt. It is unclear to what extent a private enterprise can use these grounds. Could a private enterprise collect PI to maintain its network security because its network is used by a large number of customers and it is therefore in the public interest? The other set relates to situations where the processing just needs to be 'necessary'. This covers more standard situations such as compliance with a judgment or a law, situations of epidemics and threats to public health, disaster management and breakdown of public order, and various aspects of employment. It seems unlikely that most of these grounds can be used by an enterprise to collect PI purely for business purposes.

Does consent work?

Consent has been the mainstay of privacy law for many years. But it has been realised that consent as a ground for collection and processing of PI is fraught with two main difficulties. The first is the concept of consent under the GDPR. The standards are somewhat onerous and not easy to comply with, which is why most businesses in the EU prefer not to opt for consent as the ground for processing of PI. Some of this language is present in the Bill as well, that consent must be 'freely given', 'specific', 'informed', and there must be an 'unambiguous indication of consent' through a 'clear affirmative action'.

The second is that consent is not really protective of the PI of an individual. This is because, in most cases, individuals grant consent as a matter of course either as they don't really understand the implications of the use of the PI by the data controller or as they don't really have an option to say no.

The GDPR includes the ground of legitimate interest. This means that a business can collect and process PI if it has a legitimate interest in doing so. In practice, it would need to build a case for why such processing is legitimate. To my mind, this is a better way to protect privacy even though it does not provide for a black and white solution – meaning that, it is not like consent where the individual has either given it or not. One has to evaluate whether the processing of the PI is legitimate interest of the controller.

Legitimate interest and 'reasonable expectation'

One ground in the second set is where a person provides PI voluntarily and it is 'reasonably expected' that such person would provide that PI. Is this the legitimate interest ground? It is not clear. Can one contend that what a business can reasonably expect to process personal data is the same as the business having a legitimate interest in doing so? Only time will tell how this provision would be interpreted, assuming that it enters the statute books in its current form. One wonders though, when there is a term being used globally and there is substantial jurisprudence already developed, why not use the same term rather than use a different term which may have some similarity in meaning but does not actually mean the same thing. Isn't India making life difficult for itself unnecessarily? In my view, legitimate interest is the heart of privacy law and along with necessity and proportionality is the main lever for protecting privacy. In fact, the principle of proportionality should also be called out in the legislation.

Simplistic legislation

The simplistic legislation differs substantially from the GDPR in many respects. Why did the Government not opt for a GDPR-style legislation? There are important reasons not to do so. Even though India is the fifth largest economy in the world, it has an extremely large unorganised business sector and a huge small and medium-sized enterprise sector. At the same time, with digital payments being so omnipresent, only a small handful of vendors do not transact digitally. India is also a country with a low level of privacy standards and awareness. In many ways, the government has traditionally discouraged privacy. For example, one can search for information of a director of a company on the company registry and obtain copies of the director's ID cards attached to the form filed for appointment of the director! In this scenario, a blockbuster legislation like GDPR would be hard to implement in India. It would lead to large scale disruption and non-complying businesses would live in fear of prosecution and liability.

The 'poco a poco' approach

In Italian, 'poco a poco' means little by little. I have long recommended that India commence privacy regulation with a watered down, simple legislation that sets forth the basic principles but leaves it to the data protection authority to build the law slowly, through delegated legislation. PI is ubiquitous and it is hard to imagine how PI might be used and what are the implications of such use. A hard, inflexible legislation is more difficult to cure than a delegated legislation that can be changed more easily. India also does not have a privacy ecosystem in place, with few people having sufficient expertise in the area. However, the draft law only goes half-way down this road. A key aspect of this approach is to empower the data protection authority ('DPA') to pass delegated legislation and to issue guidance papers and clarifications. While the government has some rule making power, there is little power assigned to the DPA (which is referred to as the Data Protection Boad of India) in this regard. The composition of the DPA is also not prescribed, which means the government can fill it with bureaucrats and politicians rather than individuals with domain experience. There has been criticism about the number of times the Bill uses the phrase 'as may be prescribed', but in my view, the power of delegated legislation has not been properly implemented in the Bill.

One good example of a qualitative approach to delegated legislation is the approach taken by the Telecom Regulatory Authority of India ('TRAI'). TRAI issued a consultation paper which describes the background, defines the issues, and asks the necessary questions. It also refers to the law in various countries. Relevant stakeholders and even the public then provide their inputs. TRAI examines these and issues a recommendation paper which analyses the responses and draws conclusions. It is a truly collaborative and democratic exercise which is much needed in privacy because it is so difficult to conceive of how a regulation may impact the use of PI. The approach under the EU with first the working party papers and then the reports by the European Data Protection Board are another good example of how privacy law issues need to be

dealt with. A technically savvy and extremely nimble DPA is crucial in a country like India for data privacy law to be effective and enforced.

Data localisation and transfers

The previous versions of the Bill contained substantial provisions on data localisation. The last version stated that critical data could be stored only in India while sensitive personal data could be stored outside India provided a copy was available in India. The scope of critical data would be decided by the government. This caused some anxiety among businesses who were concerned that critical data might be defined broadly and cover too much.

This approach coincided with two other trends in India. One, sectoral regulations that included data localisation provisions. In the payments sector, for instance, India's central bank, the Reserve Bank of India, decreed that all payment data needed to be stored in India only and this covered everyone in the payments ecosystem. Similar provisions started to make a presence in other regulations.

At the same time, a new concept started to develop, the idea that there is some kind of data sovereignty that exists – that a country, or rather its government, has some form of ownership over the data of the citizens of the country and such data cannot be allowed to be freely used by businesses. This resulted in two reports on non-personal data, which included the notion that non-personal data, including personal data that has been anonymised, could be forcibly shared, not just for a public purpose but with competitors in a business environment. The previous versions of the Bill in fact covered some aspects of the report on non-personal data, allowing the government to direct that anonymised personal data or non-personal data be transferred to it to enable better targeting of delivery of services and formulation of evidence based policies by the government.

These approaches appear to have fallen by the wayside as there is no data localisation in the Bill. However, with regard to data transfers, the law covers only one ground – adequacy. This seems strange given that India does not have adequacy status with the EU and most EU personal data is accessed in India through the enforcement of Standard Contractual Clauses. This is probably the result of trying to be too simplistic in drafting the legislation. However, more troubling is the fact that there does not appear to be power given to either the government or the DPA to prescribe other grounds for data transfers. They could do so through the backdoor (for those countries not meeting adequacy, other grounds can be prescribed) but theoretically, it is questionable whether that would be permitted use of delegated power.

Government exemptions

The Bill grants the right to the government to exempt the government and its instrumentalities from any provision of the law. Further, the limitations on retention (deleting the data when its retention no longer serves the purpose of collection) do not apply to the government. No safeguards like reasonableness or proportionality have been mentioned. There is a clear conflict of interest in the government being empowered to regulate itself. Exemptions to government under the GDPR are required to be passed through legislation and there are substantial safeguards prescribed. The only saving grace here is that the Supreme Court of India had held that restrictions on privacy must meet the standards of reasonableness and proportionality from a constitutional rights perspective, and therefore, whether these standards are specifically mentioned in the legislation or not, they would still apply. It is unfortunate and distressing that limitations on retention do not apply to the government. If the purpose of collection is no longer being served, I see no reason why the government cannot delete the data as well.

Other issues

There are several other key issues that need to be addressed. These include some issues relating to the definitions, a blanket requirement to notify data subjects in every instance of a data breach, and keeping the age of children at 18 years, etc. It is hope that many of these issues will be ironed out in the final draft.

Conclusion

The Bill is currently being reviewed by the Government after receiving public feedback. A revised draft will then be prepared and it is expected that that draft would be presented to Parliament for enactment. The overall approach by the Government seems right even though it may go against recent trends, but the drafting is largely substandard - there is much to be added to and corrected in the nitty gritty of the law and it is hoped that most of that will be sorted out in the next draft of the law.

Stephen Mathias Senior Partner
stephen.mathias@bgl.kochhar.com
Kochhar & Co., Bangalore

Privacy snapshot:
Regulation ramps up

As 2022 drew to a close, a look into what's going to be on policy makers' and organizations' agendas for 2023 began to emerge. International data transfers continue to be a key area of focus, as developments in this area have stolen the headlines again – the European Commission published its draft adequacy decision for the EU-US Data Privacy Framework ('DPF'), the Organisation of Economic Cooperation and Development ('OECD') adopted its Declaration on Government Access to Personal Data Held by Private Sector Entities, Binding Corporate Rules ('BCRs') were put under review by the European Data Protection Board ('EDPB'), and the UK Information Commissioner's Office ('ICO') published new transfer guidance. Staying on top of, and adjusting programs to, new regulations remains a challenge – from the US to India, organisations have been closely monitoring the trajectory of privacy laws. In Europe, the focus has begun to shift to regulating broader usages of data. The EU's Digital and Data Strategy has been under the spotlight of late, an initiative which is closer to bringing forth new abbreviations for us to familiarise with – the DGA, the DMA, the DSA, the Data Act, and the AI Act, whilst NIS2 and DORA aim to tighten cybersecurity requirements and operational resilience. Here's a round-up of where regulation has been ramping up.

International data transfers continue to make headlines

EU-US transfers

Following the Executive Order issued by President Biden at the beginning of October 2022, analysis and debate began as to how the commitments under it would impact the viability of a future data transfer agreement. The wait for the European Commission's analysis ended on December 13, when it published its draft adequacy decision for the DPF, aimed at fostering safe data flows and addressing concerns raised by the Court of Justice of the European Union's judgment in Schrems II.

As expected, the draft decision determines that the US, through the DPF, provides comparable safeguards to those of the EU and ensures an adequate level of protection for personal data transferred from the EU to certified organisations in the US.

As for what's next – the draft decision has been sent to the EDPB for its opinion. Following this, the Commission will seek approval from a committee composed of representatives of the EU Member States, and the European Parliament will also have the right to review the adequacy decision. Once this procedure is completed, the Commission will then be able to proceed with adopting the final adequacy decision. In the meantime, organisations are beginning to familiarise themselves with the updated DPF Principles should the framework get the green light.

OECD Declaration

With government access being one of the key talking points when it comes to international data transfers, 38 OECD countries and the EU announced the adoption of a major international agreement among democratic nations committing to common standards for safeguarding privacy, and assuring transparency, oversight, and redress with respect to their governments' law enforcement and national security data access.

OECD Secretary-General Mathias Cormann described the Declaration saying, "Today's landmark agreement formally recognises that OECD countries uphold common standards and safeguards. It will help to enable flows of data between rule-of-law democracies, with the safeguards needed for individuals' trust in the digital economy and mutual trust among governments regarding the personal data of their citizens."

The Declaration aims to complement the OECD's Privacy Guidelines, which date back to 1980, and which have formed the basis of many of the principles that are embedded into privacy laws today. As such, it will be interesting to see how this new Declaration will impact the trajectory of discussions around data transfers, and whether it marks the beginning of a more harmonised, global effort to address trust in data flows.

Binding Corporate Rules

BCRs were enshrined within law for the first time under Article 47 of the GDPR. Because of the legal commitments and efforts required by organisations, coupled with the fact that they require scrutiny and approval from the data protection authorities, the ICO continues to refer to their use as 'the gold standard transfer mechanism'.

In November, the EDPB opened a public consultation on its Recommendations on the application for approval and on the elements and principles to be found in Controller Binding Corporate Rules ('BCR-C'). The Recommendations intend to repeal and replace previously adopted Article 29 Working Party documents – WP256 rev.01 and WP264 – and comprise of two major sections: firstly, the detail and instructions regarding the application form for approval of BCR-C, and secondly, the elements and principles to be found in BCR-C.

Following the CJEU's decision in Schrems II, the EDPB confirmed that 'the Court's assessment applies as well in the context of BCRs, since U.S. law will also have primacy over this tool'. It's clear several updates have been made to reflect this – section 5.4.1. for example, specifically refers to the EDPB's Recommendations on measures that supplement transfer tools, and provides that there should be a clear commitment that BCR-C are only used as a tool for transfers where the law and practices in the third country have been assessed.

For existing BCR holders, there's another important call out: once finalised, the EDPB expects 'all BCR-C holders to bring their BCR-C in line' with the requirements set out in the Recommendations, including 'BCR-C that have been approved before the publication of these Recommendations'.

ICO guidance

Speaking of carrying out transfer impact assessments, the ICO weighed in with its own updated guidance on international transfers that it previously announced would be published following the publication of the International Data Transfer Addendum ('IDTA') and the Addendum to the EU's Standard Contractual Clauses ('SCCs'). The updated guidance contains a new section on transfer risk assessments ('TRA'), as well as a TRA tool.

According the ICO, its TRA guidance clarifies 'an alternative approach to the one put forward by the EDPB [which delivers] the right protection for the people the data is about, whilst ensuring that the assessment is reasonable and proportionate'.

The ICO's TRA tool contains six sections and comes with guidance to help organisations complete each. That guidance includes initial risk levels, matrices, decision trees, and examples of the technical, organisational, and contractual protections business can implement.

What's next for the ICO on data transfers? In its press release, it advised that it's working on guidance on how to use the IDTA and the Addendum to the SCCs. What will also be interesting to watch is the press release's final note that it's considering 'extending the TRA guidance to include worked examples to show how the TRA tool can work in practice'.

Keeping up and staying ahead of legislative change

The privacy landscape is such right now that it's the norm to have at least a few legislative updates and developments to discuss every month or so.

Whilst many organisations have been preparing for the entry into effect of the California Privacy Rights Act

('CPRA') and Virginia's Consumer Data Protection Act on 1 January 2023, they have also been closely monitoring the activities of the new California Privacy Protection Agency ('CPPA').

Most recently, this included requesting public comments on a revised version of its updates to the existing regulations previously issued by the Attorney General. Having already gone through some modifications, additional changes have been made in this latest version, such as to the provisions on restrictions on the collection and use of personal information, requirements surrounding opt-out preference signals and the right to opt-out of sales, and obligations of service providers and contractors. The comment period closed at the end of November, and a finalised version is expected to be released some time towards the end of January or early February 2023.

Elsewhere in the US, the Colorado Privacy Act ('CPA') is due to enter into effect on 1 July 2023, and ahead of this, the Colorado Attorney General published an updated version of its draft rules implementing the CPA in December, based on feedback that it received. Changes include updates to definitions and requirements in relation to data protection assessments, among other areas. A formal CPA rule-making hearing will take place on 1 February 2023, and written input can also be submitted.

In India, data protection legislation has been a heavily discussed issue since the Supreme Court of India's decision in the Puttaswamy case declared privacy a fundamental right in 2017. Several efforts have been made to pass a comprehensive data protection law since that time, however, the proposed bills have stumbled. In November, the Ministry of Electronics and Information Technology ('MeitY') released a new Digital Personal Data Protection Bill, launching a public consultation on this revised piece of legislation. The consultation closed on 2 January 2023, after receiving an extension, and so attention will turn to how this latest proposal will develop over the course of the year.

With data security an ever-present theme, Australia also decided to enact legislation in December to increase penalties for repeated or serious privacy breaches by companies which fail to take adequate care of customer data. The Government also emphasised that the Privacy Legislation Amendment Act provides the Office of the Australian Information Commissioner with greater powers to resolve privacy breaches and quickly share information about data breaches to help protect impacted customers. The change is in addition to a comprehensive review of the Privacy Act by the Attorney General's department, with recommendations expected for further reform of privacy legislation in 2023.

EU data regulations are coming

It's been a busy few months in the EU. Since the launch of its Digital and Data Strategies in 2020, several pieces of legislation regulating data have been put on the table. These include the AI Act, the DMA, the DSA, the Data Act, the DGA, as well as others. Both the DSA and the DMA entered into force, following on from the DGA's entry into effect earlier in 2022. Organisations subject to these new laws will be looking forwards to the laws' applicability dates over the coming two years, to build and adjust programs to new requirements. Privacy teams will be central to these efforts as the evolution from compliance to data governance becomes part of the broader strategy for strong data practices.

One of these proposals that has the potential to have a significant impact on many organisations and the way they use data and technology is the AI Act. There was much debate within the Council of the European Union on the draft text until when in early December it announced that it had adopted its general approach. The adoption means that the Council can now enter into negotiations with the European Parliament, once the latter adopts its own position.

Although considered a key part of the EU's Digital and Data Strategy, the nature of the issues which the AI Act attempts to deal with, coupled with the fact that this will represent the first major piece of harmonised legislation to regulate AI, it remains to be seen how quickly negotiations between the Council and the Parliament will be concluded.

However, that isn't the end of new regulation in the EU. In November, both the revised Directive on security of network and information systems ('NIS2') and the Regulation on digital operational resilience for the financial sector ('DORA') were adopted. NIS2 aims to bring tighter cybersecurity obligations for risk management, reporting obligations, and information sharing, whilst DORA aims to 'ensure that the EU's financial sector is more resilient to severe operational disruptions and cyber-attacks'. The broadening of organisations covered under both pieces of legislation as well as their enhanced requirements adds further dimensions for companies when assessing compliance with the EU's continued efforts to regulate the broader data and cybersecurity domains.

Alexis Kateifides CoE Program Director
akateifides@onetrust.com

Meet a DPO:

Monika Tomczak-Gorlikowska

Tell us about yourself and your role. How would you describe it and what does a 'typical' day look like?
First of all, I am very honoured to be featured in OneTrust's Data Protection Leader magazine! Let me introduce myself – my name is Monika Tomczak-Gorlikowska and I am the Chief Privacy Officer of the Prosus Group.

Prosus is a global consumer internet group and one of the largest technology investors in the world. The strategy Prosus pursues as an investor very much influences my approach to the role – we operate in a decentralised structure that empowers local leaders, backed by our group's global scale. This is different than a typical centralised global privacy program.

My role keeps me contributing to the growth of a global network of privacy leaders across the businesses we own, while fostering each respective company's adherence to our Board's overarching Group Policy on Data Privacy Governance.

My typical day involves running various initiatives at global level to make it happen – this may be a call with India businesses to discuss the impact of the future India Privacy Bill in the morning, enhancing the application of our Prosus Privacy Maturity Model at midday, and running a working group for our investments in Brazil in the afternoon... I am also responsible for making sure that, as a company listed in multiple jurisdictions, we comply with all relevant data privacy compliance requirements.

What drew you to working in data protection and privacy?
I started my adventure with privacy back in 1998 when European countries had to implement the Data Protection Directive, officially Directive 95/46/EC, in the old days! At that time in Poland/Central Europe, very few people were looking into this space and most countries did not even have privacy laws. I immediately enjoyed the cross-sectional nature of privacy and data protection. Human rights aspects, European Law, data models, marketing, international issues, loads of IT implementation, you name it... I haven't regretted it since, as data protection and privacy always require an open mind and an appetite to follow rapid technology progress.

What are the key privacy compliance areas that are top of mind for you right now for your program?
For this year and the coming ones, we are very much focusing on the following areas – first, alignment of our privacy program with the Group's strategic goals as an investor – in terms of executive reporting and communication, risk assessment and benchmarking. We are actively deploying our bespoke Prosus Privacy Maturity Model, which enables our companies to measure the maturity of their privacy programmes, set goals and prioritize their efforts. In this their capacity to comply with applicable data protection laws is assessed across 17 dimensions of privacy program management that we measure.

> ***Our privacy program is now firmly part of the Group's sustainability strategy and privacy has been identified as a material dimension in that effort***

Second, our privacy program is now firmly part of the Group's sustainability strategy and privacy has been identified as a material dimension in that effort. For instance, we will be contributing to the route to align with the requirements stemming from the new European Corporate Sustainability Reporting Directive ('CSRD').

Last but not least, we are also actively looking at the AI space and this year we continue to build out our Approach to AI Ethics. The list is not exhaustive, as you can imagine...

What are the key elements of your privacy program? Is it based on particular laws/standards/frameworks? How has it evolved over time?
The foundation of our global privacy program is the Group Policy on Data Privacy Governance (at www.prosus.com/privacy). It has been adopted by the Board and we expect all our majority owned investment companies to adhere to the seven privacy principles and implement the seven key elements of an accountable privacy program. These are well-recognised privacy principles and requirements for an efficient privacy program designed to help businesses from start-up to maturity manage privacy across different jurisdictions. These can be mapped against such laws as the GDPR, but they are deliberately jurisdiction-neutral.

At the same time, the Policy leaves our companies a high degree of flexibility about how to build such programs to accommodate different business models, resources, culture and legal requirements across the jurisdictions in which they operate.

The programs have evolved over time with the growing maturity of our companies and the rise of data privacy legal requirements, especially in jurisdictions of the global south where we have numerous investments. But fundamentally, each of our companies has its own scalable and free-standing privacy program. In alignment with the Policy, we foster best practices, grow the network of Privacy Leaders and support Group companies in the journey to mature their privacy framework.

Which other business functions do you regularly interact with, and why?
As mentioned before, our goal is to align the privacy program with the business strategy, hence the importance of executive communication. We also work very closely with our Investor Relations, Sustainability, AI, Finance, M&A, Cyber, IT, HR, Legal, Public Affairs and Communication functions.

Personally, I am a firm believer in driving the privacy program in close collaboration with others in the organisation rather than fencing off the privacy office or unilaterally driving most initiatives. This definitely contributes to the understanding that privacy is not just about compliance with privacy laws. We don't always have to be in the driving seat...

In my view, this attitude is going to be even more pertinent in the future where the regulations are data driven in a pluridisciplinary manner and the privacy office needs to be able to respond to new challenges.

What are your thoughts on the rapid pace of change within data protection and privacy? Are there any recent developments that have been of either personal or business interest?
Personally, I very much welcome the evolution of the privacy profession. I know it is challenging but the fact that we need to constantly immerse ourselves in new tech developments, such as AI, PETs, the metaverse or areas such as sustainability, keeps the thrill... The pace is indeed getting faster but so is the world around it.

The items on my favourites list are technology-related such as the rise in sophistication in Privacy Enhancing Technologies or the rapid evolution of generative AI, but I am also fascinated by the rise of privacy culture in regions of the world that have only recently adopted privacy laws or are in the process of doing so. A lot of satisfaction is derived from the opportunity to support but not impose ready-made solutions for such jurisdictions!

What advice would you give to others looking to maintain and evolve their privacy programs?
There is no universal wisdom here but in my view a few things are useful...

First, excel at communication, in particular to business leaders or strategic decision makers. This requires the understanding what they actually care about and what will make a difference to the organisation.

Second, seek allies – a lot of the goals of a privacy program align with the objectives of other functions, as mentioned before, and in fact may be driven more efficiently through more comprehensive business processes.

Third, prioritize and be able to accept the fact that the privacy program is not the only goal of your company... Surprisingly, this approach may actually help in achieving the next level where it really matters.

> ***I am a firm believer in driving the privacy program in close collaboration with others in the organisation rather than fencing off the privacy office or unilaterally driving most initiatives***

What do you think the biggest challenge facing the data protection industry at the moment is? Will this change over the next five years?
Undoubtedly, the data protection industry across the entire spectrum will need to adapt to the changes to remain relevant. New laws and strategic global initiatives are more and more being defined in areas such as AI, Data Governance, Data Economy and ESG. Privacy professionals need to be able to step outside of their comfort zone and contribute to the global data debate. This does not necessarily mean that the data protection industry needs to take over or fully absorb these areas in its scope, but sometimes also accept a seat at the table and the opportunity for a valuable contribution driven by experience from building efficient and accountable programmes.

5 MINUTES WITH...

Spiros Tassis

Spiros has been an IT Law, Data Protection, and Privacy lawyer since 1999. Spiros is a member of the Bar of Athens (Supreme Court), chair of the Hellenic Association of Data Protection and Privacy (HADPP), BoD of the EFDPO, founder and former co-chair of the #IAPP Greek Knowledge Chapter, Associate of the Department of Applied Informatics, University of Macedonia, and a member of the AI in Justice committee.

In 2010, Spiros established the Tassis & Associates Firm, which is now a leading TMT and Privacy law firm in Greece running data management and compliance projects for major entities and organisations of the private and public sector. Tassis & Associates Firm has also gained an extensive experience in eGov, cybersecurity, AI, and data related projects. Before 2010, Spiros served as Head Corporate Legal Adviser to fixed and mobile telecommunication companies.

Tell us a bit about your job role and how you have progressed in your career?
I was lucky enough to be a student in the early 90's when technology was emerging as a commodity and as something that was accessible by, almost, anyone. The advent of personal computers and the first steps of e-communications made me realise that in the future we will be forced to create a special legal framework for technology and its products; a framework that shall borrow elements from the classic law systems but that will also need to discover new legal tools to address the new social needs.

After achieving an LLM in IT and Privacy in the UK, I returned to Greece and had the chance to work for telecoms and tech companies and gain some unique experience. Now, I am leading a team of experts with a solid knowledge in our field and a very good understanding of technology and innovation. As we usually have to opinion on innovative and complex digital/tech/data issues, we must be able to quickly apply the proper legal framework and consult on all possible outcomes.

Our primary target is to secure compliance but in a business-friendly way. Our clients count on us to draft a legal strategy that will facilitate them in being proactive and be aware of the legal risks.

What alternative job would you have if you had not gone into law?
Law studies train you how to put together facts, goals, and emotions to achieve a result close to what the client is seeking. So, I find it very interesting that if I had not become a lawyer, I would be very happy as a movie director or a mathematician.

What do you love about your job, and what do you find challenging?
I genuinely love when, with my brilliant associates, we meet new clients, especially entrepreneurs in technology, have them analysing their vision and then brainstorming on how we may assist them to achieve successful business relations and materialise their challenging ideas.

Where is your favourite place on earth?
Anywhere my loved ones are and ideally in a Greek seaside village sometime in October.

Who would play you in a film about your life?
Surely not a tall blonde north-European guy...

What is your favourite book?
Every year I have a new one, but my all-time classic choices are all the mystery novels of Andrea Camilleri, the 'Theory of Justice' by John Rawls, 'Gaspard, Melchior and Balthasar' by Michel Tournier, and Aristotle's 'Nicomachean Ethics'.

What is some advice you would give to others starting off in your industry?
Be curious, dig deep into knowledge, and trust your instincts!

Who is your inspiration?
Young professionals with a fresh eye and an inquiring mind. Also, my two kids with their independent spirit and straightforward logic - they are the tech generation.

Read Spiros' latest Insight article, Greece: Bill on emerging technology - a unified framework, on the OneTrust DataGuidance platform today.

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

Email: DPL@onetrust.com