Ideas shaping privacy, published by OneTrust DataGuidance®

V7, ISSUE 4

JULY 2025

Data Protection Leader

TO REGULATE OR NOT TO REGULATE... THE ANSWER IS CLEAR

USA DEVELOPMENTS REGARDING CHILDREN'S DATA

State and federal efforts to modernize COPPA and enforce youth privacy laws

EU DMA AND GDPR

Considering overlaps in the privacy-competition landscape

COUNTRY PROFILE: PHILIPPINES

Exploring frameworks on data privacy and AI systems

onetrust DataGuidance

Contributors to this issue

Eduardo Ustaran
Partner, Hogan Lovells

Eduardo Ustaran is Global co-head of the Hogan Lovells Privacy and Cybersecurity practice and is widely recognized 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 AI and connected devices to the implementation of global privacy compliance programs and mechanisms to legitimize international data flows.

Guoda Šileikytė
Associate Partner, WALLESS

Guoda Šileikytė is a Certified Information Privacy Professional (CIPP/E) and a Certified Information Privacy Manager (CIPM). Her main legal practice encompasses data protection, privacy, technology, and digital markets. As an Associate Partner at WALLESS, she also specializes in life sciences, consumer, and commercial law. Guoda helps clients navigate through complex regulatory matters and provides pragmatic, solution-focused advice. In her day-to-day activities, Guoda evaluates companies' compliance, assists with preparation of any required documentation, conducts GDPR awareness training, and assists in preventing and reacting to data breaches.

Gene Fishel
Counsel, Troutman Pepper Locke, LLP

Gene is a former regulator with two decades of experience who has overseen state privacy and cybersecurity regulation enforcement, led national, multistate attorneys general privacy investigations, and prosecuted computer crimes at the state and federal levels. He has served at the forefront of state attorney general and federal enforcement and utilizes this experience to proficiently represent client interests. With an exemplary understanding of applying existing law to evolving cybersecurity and privacy problems, he guides clients navigating such issues and advises them at every stage of a matter.

Kyara Rivera Rivera
Associate, Troutman Pepper Locke, LLP

Kyara is an associate in the firm's Regulatory Investigations, Strategy + Enforcement Practice Group. She received her J.D. from the University of Richmond School of Law, cum laude, where she served as publications and online editor of the Public Interest Law Review.

Edsel F. Tupaz
Senior Partner, Gorriceta Africa Cauton & Saaavedra

A dual-qualified lawyer under the Philippine and New York Bars, Edsel leads the firm's Data Privacy, Cybersecurity, and AI Initiatives practice, as well as its Special Projects group. His practice covers data privacy and cybersecurity, infrastructure, TMT, banking and financial services, corporate law, government procurement (R.A. 9184), and public policy. He advises Fortune 500, NASDAQ-listed, and major Southeast Asian tech companies, and serves as DPO for leading start-ups and incumbents. Edsel also advises on fintech, crypto, e-commerce, and routinely helps clients establish a business presence in the Philippines.

Melike Hamzaoğlu
Partner, Hamzaoğlu & Partners

Melike is a highly accomplished legal professional with a broad practice spanning privacy, data protection, cybersecurity, fintech, blockchain, commercial contracts, and corporate law. Her expertise includes emerging technologies such as AI and robotics. In addition to advisory and transactional work, she leads the firm's Dispute Resolution Division, overseeing complex legal conflicts with strategic precision. Recognized for several years as a Legal 500 Recommended Lawyer in IT and Telecoms, Melike lectures on AI and technology law and regularly shares her expertise at conferences, universities, and industry events, shaping discussions on the legal and ethical challenges of emerging technologies.

Yücel Hamzaoğlu
Partner, Hamzaoğlu & Partners

Widely respected for his professional excellence, Yücel brings specialized insights in AI, cybersecurity, fintech, cryptocurrencies, telecommunications, electronic money, and online payments, helping clients navigate today's complex digital landscape. He offers deep expertise in IT, intellectual property, and data protection, taking a collaborative, client-focused approach. Beyond his legal practice, Yücel has years of academic experience lecturing on technology law, data privacy, and e-commerce. He has been recognized as a Leading Partner in IT and Telecoms in Türkiye by The Legal 500.

Batu Kınıkoğlu
Partner, Hamzaoğlu & Partners

Batu has a broad range of experience in data protection and telecommunications law and is valued by clients for his technical knowledge and dedication. He advises clients on a wide range of issues, including data protection, information privacy, cybersecurity, e-commerce, and telecommunications law. His expertise also includes copyright and open-source software licensing. Batu has articles published in international refereed academic journals on subjects ranging from copyright to internet regulation. He is a Legal 500 Recommended Lawyer in the areas of IT and Telecoms and Intellectual Property and a Who's Who Legal expert in the areas of Data Privacy & Protection and Data Security.

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

Table of contents

To regulate or not to regulate... The answer is clear
By Eduardo Ustaran, Hogan Lovells 5

California - CCPA cookie banners
By Timothy J. Toohey, Timothy J. Toohey, a Professional Corporation 6

Breaking down the walls: How the DMA and GDPR are reshaping the privacy-competition landscape
By Guoda Šileikytė, WALLESS 10

USA: Legal, regulatory, and enforcement developments regarding children's data
By Alaap Shah and Lisa Pierce Reisz, Epstein Becker & Green, P.C. 14

Virginia enacts restrictions for children on social media
By Gene Fishel and Kyara Rivera Rivera, Troutman Pepper Locke, LLP 18

Country Profile: Philippines
By Edsel F. Tupaz, Gorriceta Africa Cauton & Saavedra 22

Data transfers, their implications, and recent fines for social media companies in China
By Dehao Zhang, Fieldfisher China 26

Turkey cyberlaw - Key compliance requirements and challenges
By Melike Hamzaoğlu, Yücel Hamzaoğlu, and Batu Kınıkoğlu, Hamzaoğlu & Partners 28

Meet a DPO: Abel Kaszian
Wizz Air 28

5 minutes with: Marton Domokos
Partner, CMS 28

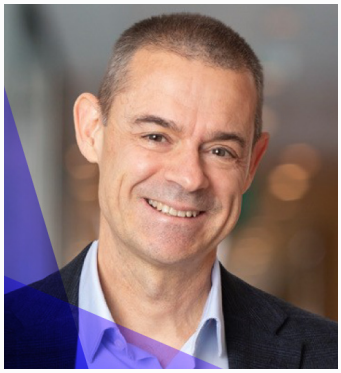
Cover page: George Hammerstein/The Image Bank via Getty Images, Page 4: Travel Wild/iStock via Getty Images, Pages 6-7: SEAN GLADWELL/Moment via Getty Images, Pages 8-9: John M Lund Photography Inc/DigitalVision via Getty Images, Pages 10-11: EschCollection/DigitalVision via Getty Images, Pages 12-13: ThamKC/iStock via Getty Images, Pages 16-17: The Good Brigade/DigitalVision via Getty Images, Pages 18-19: peeterv/iStock via Getty Images, Page 21: Alexander Spatari/Moment via Getty Images, Pages 22-23: KTSDESIGN/SCIENCE PHOTO LIBRARY/Science Photo Library via Getty Images, Pages 26-27: Angel Santana/Moment via Getty Images, Pages 30-31: Cravetiger/Moment via Getty Images, Pages 32-33: Yaroslav Kushta/Moment via Getty Images, Pages 34-35: Antonio Hugo Photo/Moment via Getty Images.

Editor: Eduardo Ustaran | eduardo.ustaran@hoganlovells.com
Managing Editor: Alexis Kateifides | akateifides@onetrust.com
Editorial Lead: Victoria Prescott | vprescott@onetrust.com
Editorial Staff: Cristina Die González | cristina.die@onetrust.com - Isabelle Strong | isabelle.strong@onetrust.com

Editorial

Digital governance that is attuned to technological opportunity and alert to potential harms is the obvious answer to one of the most existential questions of our time.

Editorial: To regulate or not to regulate… The answer is clear



Not to be overdramatic, but governments' Shakespearian dilemma over how to strike the right balance between a regulatory approach that promotes digital innovation and one that effectively addresses the potentially devastating risks of artificial intelligence (AI) technology is taking on existential dimensions. Mixed messages, legislative flip-flopping, and regulatory inconsistencies are all contributing to a sense of uncertainty for both industry and citizens. And while pretty much everyone agrees that the fast pace of technological development is unstoppable, there is a degree of paralysis affecting corporate decisions about the right approach to digital governance. To move forward, paying attention to what is really happening on the data and AI regulatory front, and understanding the mindset and actions of policymakers and regulators beyond the hype, is key. The good news is that the clues are all out there.

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

Let's start with the latest regulatory attitudes towards existing laws. The ever-prolific European Data Protection Board (EDPB) has issued a 13-page detailed assessment of the European Commission's proposed simplification of the requirement to maintain a record of processing activities under the General Data Protection Regulation (GDPR) for SMEs. The ChatGPT spot-on one-sentence summary of the EDPB's conclusion is that while it supports simplifying recordkeeping obligations for SMEs, any exemptions must be clearly defined and proportionate and must not compromise data protection rights. What ChatGPT is not saying is that, compared to the immensity of the GDPR, this is like debating the pros and cons of rearranging the deck chairs on the Titanic. Or in other words, don't expect a radical (or even relatively minor, as the UK has done) reform of the European data protection framework any time soon.

Perhaps the most consequential development in European digital regulation right now is the implementation of the AI Act, with its staggered rollout of obligations that started at the beginning of this year and will continue until the summer of 2027. However, partly due to its novelty and partly due to political pressures, there has been some perceived hesitation among policy power players about how to position this hugely ambitious framework. The response from the European Commission has been a balanced blend of reasonableness and robustness. The reasonableness is best evidenced by the openly supportive attitude exhibited by the AI Office towards any provider of general-purpose AI (GPAI) models that is willing to assert its credentials as a responsible AI developer by adhering to the GPAI Code of Practice. But while the Commission may be prepared to be patient and understanding, it is by no means conceding on its commendable quest to ensure that the development and deployment of AI is safe, secure, and above all, compatible with fundamental rights. So, the AI Act is definitely here to stay.

At the same time, amid all the cacophony emanating from the other side of the Atlantic, a picture is emerging of how the US is approaching the AI regulatory landscape. The White House 'AI Action Plan' has a lot to unpack, but the Trump Administration's basic message when it comes to AI regulation is pretty straightforward: remove red tape and onerous regulation. What is less clear-cut is what this means in practice when, at the same time, a number of individual states are actively seeking to pass AI-specific laws, and Congress voted overwhelmingly against a moratorium that would have imposed a 10-year ban on states enforcing their own AI laws. So in reality, even the US Federal Government is acknowledging that it should not interfere with states' rights to pass prudent laws that are not unduly restrictive to innovation.

Where does this leave us? Certainly not in a lawless environment. Digital regulation is evolving in the same way that technology itself is evolving. Policymakers are keen to show their pro-innovation credentials and call out unnecessarily burdensome laws that deliver little more than paperwork. But the need for responsibility and accountability remains, and regulators' commitment to doing their job is unlikely to fade. There will be some wavering, and unprincipled policies will be pursued, but on the whole, the direction is set and it is not towards an 'undiscovered country.' Digital governance that is attuned to technological opportunity and alert to potential harms is the obvious answer to one of the most existential questions of our time.

California - CCPA cookie banners

Timothy J. Toohey
Founder and Partner
tim@tjtooheylaw.com
Timothy J. Toohey, a Professional Corporation, California

Some years ago, the public began to confront annoying banners that popped up on websites acting as a digital Cerberus, preventing entry onto the website unless the user signaled consent for the use of various 'cookies.' Although language varies widely, a typical banner stated: "We use cookies to optimize your browsing experience for the purpose of personalizing and measuring the effectiveness of ads. By clicking 'Allow All,' you consent to our use of cookies."

For the few who somehow remain uninitiated, 'cookies' are small files embedded in a website that perform various functions (like bit players in a Shakespeare play), including tracking in various ways the actions of the user on the website. The name is taken from an earlier programming term for a small data file.

Like other privacy-protective phenomena, cookie banners stem not from the fragmented US privacy landscape but from Europe. Despite their ubiquity today on US websites, the 'cookie banner' as such is not required under any US privacy law. The reason for this stems from the prevailing tendency of US law generally not to require consumer consent for the collection of personal information.

In their origin, which stems from the prehistoric era of the EU Privacy Directive of 2002, cookie banners were based on an opt-out model. From 2009, cookie banners, consistent with the EU's General Data Protection Regulation (GDPR), required opt-in consent for EU data subjects. The difference between the EU's opt-in and the prevailing US model is sometimes overlooked, but it is a significant source of confusion that exists when considering cookie banners under US law, including that of California.

In 2018, 16 years after cookie banners first emerged in the EU, California passed its Consumer Privacy Act (CCPA), as amended by voters in 2020 through the California Privacy Rights Act (CPRA). California now has its own privacy regime, which bears some similarities to that of the EU. For example, the CCPA is enforced by the California Privacy Protection Agency (CPPA), which resembles a European data protection authority, and which enforces (as do its European counterparts) a substantial body of regulations. However, significant differences remain with the EU's GDPR. 'Consumers' under the CCPA are generally not required to consent to data collection, but only to receive notice of collection practices. Consumers only have an opt-out right that is limited to the sale or sharing of their personal information for cross-behavioral marketing purposes, i.e., for targeted advertising with third parties.

Confronted with the requirement of having to provide for consumer opt-out of targeted advertising, which is typically implemented through cookies, some companies subject to the CCPA have decided to place this opt-out right in a cookie banner along with consumer options to opt out or accept other cookies, which is a practice imported from the EU.

Until recently, business entities subject to the CCPA had little or no official guidance in California for the use of cookie banners, which is not surprising given that cookie banners are not a requirement under the CCPA. However, to the surprise of some observers, who had not seen that the issue was on its radar screen, the CPPA in a March 7, 2025 decision addressed an aspect of cookie banners as part of a more general decision addressing other issues, including consumers' verification of themselves for certain rights, the verification of authority of agents, and sharing personal information with vendors. The CPPA's order of decision, accompanied by a stipulated final order, arose in a case involving an automobile

manufacturer and distributor (the Company) that had provided consumers a choice mechanism in a commonly used format sometimes called a cookie management tool (or CMT). As a consequence of the CPPA's decision regarding the Company, entities subject to the CCPA will need to review their cookie banners and CMTs, including those similar to the ones used by the Company.

The Company's CMT provided a menu of consumer privacy choices. The Company's website form included not only an option to indicate consent or refusal for the placement of more traditional cookies, such as 'performance cookies' and 'functional cookies,' but also for what the Company called 'advertising cookies.' According to the Company's CMT, 'advertising cookies' were set by the Company or its 'advertising partners' and were used 'to build a profile of your [the consumer's] interests and show [the consumer] advertisements on other sites that we or these third parties believe would be relevant to you.' As the CPPA found, 'advertising cookies' on the Company's website were meant to provide the consumer with the option granted by the CPPA to opt out of the sale/sharing of the consumer's personal information for cross-context behavioral advertising.

Cookie banners are not the only or most typical means of providing consumers with this right. Many entities provide a link to a separate button or toggle switch to allow consumers to opt out of sale/sharing of information from a section on the website landing page titled something like 'do not share or sell my personal information.' Neither the CCPA nor its implementing regulations require a specific form of notice. Indeed, the California Department of Justice webpage on the CCPA notes only that businesses must provide a 'clear and conspicuous' link on their website that allows for an opt-out request. The AG's website also notes that consumers who cannot find the link may report the business to its office.

Focusing on the opt-out choice for advertising cookies, the CPPA found that the Company's CMT violated the CCPA in several respects. The CPPA found that the cookie banner violated Section 7004 of the California privacy regulations by not being symmetrical in consumer choice. The CPPA noted that 'symmetry in choice means that the path for a Consumer to exercise a more privacy-protective option cannot be longer or more difficult or time-consuming than the path to exercise a less privacy-protective option because that would impair or interfere with the Consumer's ability to make a choice.' In regard to the Company's 'advertising cookies,' the CPPA found that the request to opt out of the sale/sharing required more steps than the process to opt in to the sale/sharing. A consumer who opted out of the Company's advertising cookies had to go through two steps, i.e., clicking on the toggle button to the right of 'advertising cookies' and then clicking on a 'confirm my choices' button at the bottom of the banner. To opt back into advertising cookies, the consumer needs to take only one step, i.e., clicking on the 'allow all' button.

The CPPA further noted that Section 7004(a)(2)(C) of the CPPA regulations provided other examples of choices that were not symmetrical, including 'accept all' and 'more information' or 'accept all' and 'preferences.' In contrast, the choice between 'accept all' and 'decline all' was symmetrical.

Although the CPPA's guidance regarding cookie banners relates specifically to opting out of the sale/share of advertising information, it has broader implications for the numerous businesses which have implemented a CMT similar to that of the Company. Although businesses understandably may wish to conserve website 'real estate' through a privacy center which has multiple purposes, use of that option may complicate compliance with the CPPA's ruling and guidance.

Cookie banners have also become more prevalent in recent years because some businesses are using them to obtain consumer consent to their privacy practice in an attempt to prevent purported class actions under the California Invasion of Privacy Act (CIPA). As has been the subject of prior articles, plaintiffs' attorneys in recent years have brought a raft of lawsuits under CIPA and similar laws alleging that advertising cookies and pixels have been implemented on a website without the consumer's consent and that the information collected through such cookies constitutes 'surveillance' under CIPA. Seeking to avoid these lawsuits, some businesses have attempted to require consumer consent through cookie banners to implement these cookies.

The effectiveness of the use of consumer consent as a means to prevent CIPA lawsuits is uncertain. For example, questions have arisen whether obtaining (or in some cases, requiring) consent to behavioral cookies can effectively inoculate a business from a CIPA claim. In many instances, a consumer may already have been subject to a website's tracking cookies before being asked to consent to such cookies through a cookie banner. Moreover, the effectiveness of consumer consent to a privacy policy (the purpose of which is primarily one of notice) may be challenged by plaintiffs and their attorneys.

Cookie banners have had an odd trajectory. Born in a far different legal environment of the EU, which generally requires consent to the collection of personal information, they have transformed themselves in the California sun to a mechanism to implement a limited opt-out right and to forestall lawsuits involving certain cookies and pixels. Businesses using cookie banners should carefully study the recent decision by the CPPA to determine whether it impacts their current practices, particularly as to whether the options provided to consumers are symmetrical.

Breaking down the walls: How the DMA and GDPR are reshaping the privacy-competition landscape

Guoda Šileikytė
Associate Partner
guoda.sileikyte@walless.com
WALLESS, Vilnius

The recent wave of enforcement actions by the European Commission marks an important shift in EU digital regulation. For the first time, the Digital Markets Act (DMA) has been enforced against practices that sit squarely at the intersection of competition law and data protection. The Commission imposed large fines on a technology company for its app marketplace steering restrictions and a social media company over its controversial consent-or-pay models. These landmark decisions signal a new regulatory paradigm where competition and privacy considerations increasingly overlap and sometimes collide.

The rise of pay for privacy and its regulatory challenges

In November 2023, a social media company unveiled its consent-or-pay model across the EU, offering users the choice to either consent to cross-service data tracking for personalized advertising or pay a monthly subscription fee for an ad-free experience. Under the DMA, which aims to ensure fair and contestable digital markets, gatekeepers must obtain effective consent before processing personal data across platform services. Meanwhile, the General Data Protection Regulation (GDPR) requires that consent be 'freely given,' which becomes questionable when the alternative is paying. This also correlates with the DMA statement that not giving consent should not be more difficult than giving consent.

The European Data Protection Board (EDPB) addressed this in April 2024, expressing significant concerns about such model: 'In most cases, it will not be possible for large online platforms to comply with the requirements for valid consent, if they confront users only with a choice between consenting to processing of personal data for behavioral advertising purposes and paying a fee.' We can raise a fundamental question: If privacy is a human right, should people have to pay for it? So, can a model that makes privacy protection contingent on financial means be considered lawful?

Understanding the app marketplace steering case and its impact

The Commission's ruling against a technology company for its app marketplace steering restrictions highlights a key DMA priority: allowing app developers to inform users about better deals in other app marketplaces. Article 5 of the DMA clearly states that 'the gatekeeper shall allow business users, free of charge, to communicate and promote offers, including under different conditions, to end users acquired via its core platform service or through other channels, and to conclude contracts with those end users, regardless of whether, for that purpose, they use the core platform services of the gatekeeper.' Despite this, the technology company in this case created roadblocks that made this difficult in practice.

The Commission found that the company's restrictions were unnecessary and unfairly maintained its control over how users spend money on apps. Unlike the social media company case discussed above, which focused on consent for data use, the technology company's violation centered on blocking fair competition by preventing developers from simply communicating with their customers about alternative payment options. The substantial fine imposed on the company underscores the Commission's commitment to enforcing the DMA and preventing practices that undermine the goal of opening up digital markets.

These cases demonstrate how the DMA targets different types of gatekeeper behavior that limit user choice and market fairness.

Push for interoperability

The DMA also tackles another key issue: interoperability, the ability of different systems to work together. Without it, tech giants can use their control of key features to block competition and trap users in their ecosystems. In September 2024, the Commission started proceedings to help a technology company comply with interoperability requirements for certain features, particularly those used for connected devices like smartwatches and headphones. The Commission is also monitoring a social media company's progress in making messaging platforms work with other messaging apps.

This focus on interoperability aims to prevent gatekeepers from using their 'dual role' - being both a platform provider and a competitor on that platform - to favor their own products. The DMA explains that gatekeepers can also have a dual role as developers of operating systems and device manufacturers, including any technical functionality that such a device may have. Based on DMA recitals, if a gatekeeper uses its position in multiple roles in a way that blocks or limits other companies from accessing the same operating systems, hardware, or software features that it uses for its own products, this can harm competition. It can stop other developers or hardware makers from innovating and reduce choices for users.

To prevent this, gatekeepers are required to:

- let other companies access and use those same features (like parts of the operating system or hardware);
- make this free of charge; and
- ensure effective interoperability (competitor's products can work just as well with the gatekeeper's system as the gatekeeper's own products do).

This rule also applies to apps or services that support or are closely connected to the gatekeeper's main platform, so they can function smoothly and fairly alongside the gatekeeper's own apps or services.

The main goal is to make sure competitors can connect to the gatekeeper's system just as easily as the gatekeeper does (e.g., using APIs, interfaces, or other connection methods). This allows users to have real choices and encourages more innovation. Of course, the DMA sets out rules, but creating regulations is the easy part; actually implementing them takes time, resources, and a lot of effort.

The dual regulatory landscape

The DMA establishes clear criteria for identifying gatekeepers - an undertaking providing core platform services such as online search engines, online intermediation services, and social networking services (app marketplaces and messaging applications). The DMA also imposes specific obligations designed to limit gatekeepers' market power. Under Article 5 of the DMA, gatekeepers must implement measures enabling users to choose whether their data can be combined or cross-used across services. Consequently, the Commission found that a pay-or-consent model is not compliant with the DMA.

In parallel, the GDPR's consent idea requires that user permission be freely given, specific, informed, and unambiguous. Until now, various national data protection authorities have already scrutinized pay-or-consent models, arguing that financial pressure effectively coerces users into accepting data practices they might otherwise reject.

This creates a complex regulatory environment where platforms might satisfy one regulatory regime while potentially violating another. A particularly challenging aspect is that while the DMA requires consent for certain data processing activities, it does not define consent in the same detailed manner as the GDPR, creating a potential gap between complying with the letter versus the spirit of these interconnected regulations.

Growing risk of regulatory fragmentation

The institutional architecture of EU digital regulation adds extra complexity. The Commission serves as the sole enforcer of the DMA, creating a centralized enforcement regime. In contrast, the GDPR operates through a decentralized network of national data protection authorities coordinated by the EDPB.

Such a split system creates several practical challenges, such as:

- a data processing model deemed acceptable under DMA standards by the Commission might subsequently face sanctions from national data protection authorities under GDPR requirements;
- companies might strategically engage with different regulatory bodies to secure favorable interpretations, exploiting gaps between the frameworks; and
- without coordinated approaches, similar practices might face different enforcement outcomes across EU Member States.

This landscape creates significant uncertainty. For instance, a gatekeeper's

technical interoperability model might receive the Commission's approval only to face GDPR challenges from national authorities.

Concluding remarks

The cases discussed above show more than isolated enforcement actions; they signal a new regulatory world where competition law and data protection increasingly overlap. The central question is whether digital rights like privacy should be subject to market forces at all, or whether they are basic protections that cannot be priced.

Recognizing these tensions, the EDPB and the Commission have committed to developing joint guidance on the interplay between the GDPR and DMA. This collaboration is crucial for establishing regulatory coherence across the digital governance landscape. First of all, it will require harmonized interpretations to develop consistent standards for what constitutes valid consent across both regulatory frameworks.

For businesses operating across European digital markets, this evolving landscape demands a holistic compliance strategy that anticipates how different regulatory regimes might evaluate the same practices. Fairness and respect for both market competition and meaningful personal data protection should be key goals for businesses. Companies that recognize this early will be better prepared to succeed in Europe's increasingly regulated digital world.

USA: Legal, regulatory, and enforcement developments regarding children's data

Alaap Shah
Member of the Firm
abshah@ebglaw.com
Epstein Becker & Green, P.C., Washington, DC

Lisa Pierce Reisz
Attorney
LPierceReisz@ebglaw.com
Epstein Becker & Green, P.C., Washington, DC

Introduction

Protecting the digital lives of children in the United States remains a bipartisan concern and continues to be prioritized at the state and federal levels as regulators seek ways to modernize privacy rules in response to new technologies, data-driven business models, and rising social concerns. As minors increasingly interact with digital ecosystems - including social media platforms, artificial intelligence (AI) chatbots, educational apps, and content recommendation engines - the vulnerabilities of children to data exploitation and manipulation have become a central issue for lawmakers.

In recent years, federal and state legislatures, regulators, and enforcement authorities have taken numerous steps to enhance oversight of how children's data is collected, processed, and shared. These legal shifts reflect a growing consensus that the Children's Online Privacy Protection Act (COPPA), first enacted in 1998, is insufficient in isolation to protect minors in today's complex digital environments. In response, both Congress and the Federal Trade Commission (FTC) have sought to modernize COPPA's reach, while a growing number of states remain active by enacting parallel or supplementary privacy laws focused on the protection of minors.

This article surveys the latest developments in US children's privacy law, focusing specifically on enforcement trends and the implications of recent federal and state regulatory updates. It examines the rise of age-appropriate design mandates, heightened data handling obligations, biometric protections, and the expanding role of state attorneys general (AGs).

State enforcement developments: From legislation to litigation

Age verification and platform accountability

One of the most prominent themes in recent children's privacy legislation is the imposition of age verification and parental consent mandates for social media and other digital platforms. State statutes enacted in Florida, Georgia, Tennessee, and Utah in 2024 and 2025 are prime examples of this movement. Florida's Social Media Safety Act, for example, prohibits children under 14 from creating accounts and mandates parental consent for users aged 14 or 15. Enforcement mechanisms include monetary penalties and injunctive relief, with state AGs empowered to bring civil actions.

Similarly, Tennessee's Protecting Children from Social Media Act authorizes parental monitoring and consent dashboards, signaling a shift toward operational transparency and family-level oversight. States such as Georgia and Utah have added requirements for age verification on both personal and school-issued devices, further broadening the scope of compliance responsibilities for platforms.

While these laws aim to mitigate online harms such as addiction, exposure to adult content, and data misuse, their enforcement

has been uneven due to ongoing litigation challenging the constitutionality of such laws. By way of illustration, in *NetChoice v. Bonta*, the Ninth Circuit blocked provisions of California's design code law, finding potential First Amendment violations. Meanwhile, Utah's age verification laws are currently stayed pending similar litigation in *NetChoice, LLC v. Reyes*, which is currently under appeal before the U.S. Court of Appeals for the Tenth Circuit. Nonetheless, the existence of legal challenges has not deterred states from adopting increasingly aggressive regulatory postures.

Age-appropriate design codes and risk mitigation

States are also embracing design-centric regulatory frameworks modeled on the UK's Age Appropriate Design Code. California's Age-Appropriate Design Code Act requires platforms likely to be accessed by children to assess and mitigate risks to minors, conduct Data Protection Impact Assessments (DPIAs), and minimize personal data collection. Although parts of the law have been enjoined, its enactment has influenced all DPIAs, consent management protocols, and Privacy by Design mechanisms.

Enforcement under these design codes will largely depend on investigatory powers and prosecutorial discretion. Maryland's Age-Appropriate Design Code Act (the Kids Code), for instance, bans the use of geolocation data and manipulative features (e.g., autoplay, endless scroll) for children, and empowers the State's consumer protection division to initiate investigations. However, enforcement of the Maryland Kids Code remains stalled due to ongoing litigation in *NetChoice vs. Gruhn*, which alleges the law's requirements, including conducting DPIAs, violate the First Amendment.

Further, even if enforcement were to proceed at the State level, the absence of a federal law preempting State law indicates enforcement across states will vary in frequency and approach. Yet, the common trend is unmistakable: State regulators are taking a front-line role in defining and policing child-centric privacy standards.

Restrictions on harmful content and liability exposure

A parallel trend is the enactment of laws requiring platforms to verify users' ages before granting access to adult or harmful content. As of 2025, 19 states have adopted such statutes. These laws impose civil liability on platforms that fail to implement 'commercially reasonable' verification procedures.

Texas' HB 1181 - currently under review by the U.S. Supreme Court in *Free Speech Coalition, Inc. v. Paxton* - may become a landmark case for determining the constitutional limits of content-based regulation involving minors. If upheld, the decision could open the door for more aggressive state enforcement strategies targeting not just adult content but a broader range of online harms.

Federal enforcement: Modernizing COPPA

Revisions to the Children's Online Privacy Protection Rule

Recognizing the evolving threat landscape, the FTC finalized significant amendments to the Children's Online Privacy Protection Rule in January 2025. These updates modernize COPPA's core definitions and compliance obligations to address biometric data, AI-powered systems, and platforms serving both child and adult audiences.

Key changes include:

- expanded definition of personal information: COPPA now includes biometric identifiers such as facial recognition, voiceprints, and genetic data, reflecting a broader understanding of how children's identities can be exploited by emerging technologies;
- mixed audience requirements: Platforms must implement neutral age screens and are prohibited from encouraging falsification of age, closing a major loophole that previously allowed platforms to avoid COPPA by claiming not to be 'directed to children;'
- parental consent mechanisms: The rule introduces stricter standards for verifying parental consent, including multi-step authentication, mail-in forms, and voice verification methods; and
- Safe Harbor reforms: The FTC tightened requirements for COPPA Safe Harbor programs, emphasizing transparency, independence, and reduced conflicts of interest, and these reforms aim to restore public confidence in self-regulatory compliance programs.

These changes expand the FTC's enforcement toolkit and bring COPPA closer to parity with international frameworks like the EU General Data Protection Regulation (GDPR), while retaining its core US principles of notice, consent, and limited data collection.

Enforcement actions and penalties

Over the last several years, the FTC has also demonstrated renewed commitment to enforcing children's privacy rules through high-profile settlements under COPPA.

- In January 2025, the FTC settled with a video game developer for alleged violations of COPPA. The FTC alleged that the company deceived children and other users about the real costs of in-game transactions and the odds of obtaining rare prizes. Under the terms of the settlement, the company agreed to pay $20 million and to block children under 16 from making in-game purchases without parental consent.
- In July 2024, the FTC and the State of California alleged that a technology company participated in deceptive and unfair practices in violation of federal and state law (including COPPA) in

the development, design, marketing, distribution, sale, and operation of their anonymous messaging app. The complaint alleges that the company not only actively marketed its service to children and teens, but that it also falsely claimed that its AI content moderation program filtered out cyberbullying and other harmful messages. It also alleges that the defendants sent fake messages that appeared to come from real people and tricked users into signing up for their paid subscription by falsely promising that doing so would reveal the identity of the senders of messages. To settle, the company agreed to pay $5 million and is banned from offering its app to anyone under the age of 18.

- In January 2024, the FTC secured a $275 million penalty for COPPA violations by a major online gaming company, including unauthorized data collection and inadequate parental consent mechanisms. The settlement also imposed comprehensive data governance reforms.
- In June 2023, a technology company from Washington agreed to pay $20 million to settle FTC charges that it violated COPPA by collecting personal information from children who signed up for one of its gaming systems without notifying their parents or obtaining their parents' consent, and then by illegally retaining children's personal information. As part of the settlement, the company was required to strengthen its privacy protections for child users of its gaming system.
- Less than a week earlier, in a separate 2023 action, the FTC fined an e-commerce company $20 million for allowing unauthorized in-app purchases by children, reinforcing the agency's position that user interface design choices can amount to deceptive practices when they exploit minors' lack of understanding.

These enforcement actions signal that monetary fines will be paired with mandated operational reforms, including independent audits, data deletion requirements, and the implementation of child-specific controls. The FTC's strategy reflects an effort to shift from reactive enforcement to proactive structural change.

The rise of state AGs in enforcement

Perhaps the most consequential enforcement trend in children's privacy law is the emergence of state AGs as pivotal enforcers.[1] No longer content to rely solely on federal regulators, states are pursuing independent investigations and lawsuits grounded in both newly enacted statutes and general consumer protection laws.

State-level enforcement examples

- On April 29, 2025, the Michigan AG filed a lawsuit against a technology company from California, alleging that it collects and processes, and allows third parties to collect and process, children's personal information, including voice recordings, location data, IP addresses, and browsing histories, in violation of COPPA. It also alleges that the company monetizes children's personal information to increase its advertising revenue and to make its platform more attractive to content providers and advertisers. Finally, the complaint asserts that the company misleads parents about its collection of their children's personal information and creates confusion about parents' rights to protect such information.
- On March 7, 2025, New York AG Letitia James reached a settlement with a software company from New York for $650,000 to resolve alleged privacy violations involving their social networking app geared towards high school students. The complaint alleged that the company represented that it would verify users' school email credentials to ensure that the app did not allow non-students to join, and only users from the same school could interact with each other on the app. However, the NY AG determined that the company stopped authenticating email credentials, allowing users from different high schools to message each other and non-students to access almost all app features. The AG alleged that the company's practices amounted to fraudulent and deceptive trade practices in violation of New York Executive Law §63(12), the New York General Business Law, and Section 5 of the FTC Act.
- In December 2024, Texas AG Ken Paxton launched investigations under the Securing Children Online through Parental Empowerment (SCOPE) Act into into companies deploying AI chatbots that interact with minors, citing risks of emotional manipulation and data misuse.
- California AG Rob Bonta reached a $500,000 settlement with a games publisher company from New York for COPPA and CCPA violations related to their collection and sharing of children's personal information without parental consent in one of their mobile app games. The California AG's office determined that the company's age verification methods failed to encourage users to enter their age accurately and simply defaulted to older ages, that it misconfigured third-party software development that did not limit the collection, disclosure, and use of personal data based on age or consent, and that its advertising was deceptive and unlawfully targeted minors. In addition to the monetary fine, the company was subject to injunctive terms to ensure legal data collection and disclosure and diligence in configuring third-party software in their mobile games.
- In New Mexico, AG Raul Torrez filed a lawsuit against a social media company from California on September 5, 2024, to protect children from sextortion, sexual exploitation, and harm. In the lawsuit, the New Mexico Department of Justice (DOJ) alleged that the company's policies, seemingly ephemeral content, and recommendation algorithm foster the sharing of child sexual abuse material and facilitate child sexual exploitation. The New Mexico DOJ also alleged that the company's executives have misled the public about the platform's safety with ads declaring that the platform is 'more private' and 'less permanent' than other social media platforms.

While enforcement challenges persist, these enforcement powers are not merely symbolic. In the aggregate, they introduce a decentralized, multi-jurisdictional compliance risk for companies operating nationally. Businesses that once relied on harmonized federal standards must now navigate a fragmented enforcement landscape where failure to comply with one state's rule may trigger broader scrutiny.

Conclusion

Children's privacy law in the United States is undergoing continuous evolution driven by new state statutes, federal rulemaking, and unprecedented enforcement momentum. The convergence of legislative focus on protecting children, regulatory updates, and heightened litigation risk requires digital platforms to reassess how they engage with young users.

While federal amendments to COPPA provide a renewed baseline for compliance, the true frontier of enforcement lies in state-level action and the application of privacy principles to emerging technologies like AI and biometrics. Companies operating in the youth digital market must now contend with a patchwork of substantive obligations, increasing enforcement risks, and a rising expectation for transparency, consent, and Privacy by Design.

Above all, the evolving regulatory landscape signals a clear policy direction: Safeguarding children's digital lives is no longer optional; it is a legal imperative.

[1] It should be noted that on March 7, 2024, a bipartisan coalition of 43 state AGs sent a 19-page letter to the FTC with detailed comments on the FTC's January 2024 Notice of Proposed Rulemaking. Although the FTC published the Final Rule updating COPPA on April 22, 2025, making the updates effective on June 23, 2025 (with a compliance date of April 22, 2026), the detail in this letter certainly highlights the thinking of 43 state AGs who have taken an active role in the enforcement of COPPA and may be helpful to entities trying to navigate state-level enforcement efforts.

DataGuidance

WEBINAR SERIES

AI & privacy in practice:

Navigating AI's impact on business, compliance, and consumer trust

View webinar series on demand

Virginia enacts restrictions for children on social media

Gene Fishel
Counsel
gene.fishel@troutman.com
Troutman Pepper
Locke, LLP, Virginia

Kyara Rivera Rivera
Associate
kyara.riverarivera@troutman.com
Troutman Pepper
Locke, LLP, Virginia

On May 2, 2025, Virginia Governor Glenn Youngkin signed bipartisan legislation that restricts social media usage for minors younger than 16. The law takes effect on January 1, 2026, and will have a sweeping impact on companies owning or operating platforms with social media capabilities that operate in Virginia.

The bill creates a new section within the Virginia Consumer Data Protection Act directed at social media platforms with new duties and prohibitions related to minors. According to §59.1-577.1 of the Virginia Code, social media platforms must:

- use 'commercially reasonable methods' to verify whether a user is a minor - 15 years of age or younger; and
- if the user is a minor, limit the minor's usage to one hour per day, unless the parent provides their consent to increase or decrease that daily limit.

In addition to these new responsibilities, qualifying platforms must ensure that the quality of their services remains the same, regardless of the number of minors who would now have limited time on the platform.

The Attorney General of Virginia is empowered to investigate and enforce the above provisions, and violations can result in a maximum penalty of $7,500 per violation, regardless of whether the violation was intentional. The Attorney General can also impose injunctive measures that mandate changes in business practices. The law does not authorize a private right of action for violations.

Impacted businesses

The law defines a social media platform as 'a public or semipublic internet-based service or application' that has the following characteristics:

- has users in Virginia;
- allows users to connect socially within the platform;
- allows users to create public or semipublic profiles to use the platform;
- displays a public list of a user's mutual connections on the platform; and
- allows users to develop or post content for those users to view.

A public or semipublic internet-based service or application is thus considered a social media platform if it contains all of the above five characteristics.

The statute does carve out exceptions that exclude certain companies from its purview. Services and applications that offer solely messaging functions do not qualify as social media platforms based on that function alone. Additionally, platforms that consist of preselected media, such as news, sports, and entertainment that are not developed by users and where users do not post their own content, are also not social media platforms.

Virginia joins other states

Virginia joins a minority of states that have passed statutes aimed at regulating minors' social media usage. These statutes differ in their approaches. Recent state laws in Louisiana, Tennessee, and Georgia

implement age verification requirements, limit or prohibit targeted advertisements on minors' accounts, and require parental control measures. Companies must thus be aware of an increasing patchwork of state social media laws and plan accordingly.

Louisiana's Secure Online Child Interaction and Age Limitation Act (La. Stat. Ann. §51:1751 et seq.) primarily focuses on requiring social media platforms to implement age verification procedures and parental control measures on minors' accounts, while also prohibiting social media platforms from displaying targeted advertisements on those accounts. Like Virginia, Louisiana requires that social media platforms use commercially reasonable efforts to verify users' ages. If a platform fails to do so, then the statutory restrictions aimed at minors apply to all users of the platform. Additionally, covered companies must restrict any minor under the age of 16 from creating an account, unless their parent or guardian consents. Parents must also be provided with the ability to supervise their minor's account by viewing the privacy settings, setting daily usage restrictions, and setting periods of time when the minor cannot use the account. Finally, platforms operating in Louisiana cannot push advertisements based on minors' personal information and, if the platform has more than one million global users, it cannot display any targeted advertisements to minors.

Tennessee enacted the Protecting Children from Social Media Act (Tenn. Code. Ann. § 47-18-5701 et seq.) which also focuses on implementing age verification requirements on social media platforms and provides parents or guardians with greater access to monitor their minor's accounts. As in Louisiana, social media platforms must verify users' ages when they create an account, and if the user is a minor, then the platform must obtain consent from the minor's parent or guardian. However, unlike definitions in Virginia and Louisiana, a 'minor' in Tennessee is defined as any person under the age of 18. The platform must also provide the parent or guardian with the authority to revoke consent at any time and must provide them with various means to supervise the account.

As in the above states, Georgia's social media law (Ga. Code Ann. § 39-6-1 et seq.) focuses on age verification efforts and requires parental controls and advertisement prohibitions on minors' social media accounts, with a minor defined as a person under the age of 16. Similar to Louisiana, Georgia requires that social media platforms either utilize commercially reasonable efforts to verify the age of each user or apply the statutory safeguards to all user accounts. Georgia also requires parental consent for a minor to open an account and prohibits platforms from utilizing a minor's personal information for advertising purposes or collecting more information than is necessary or relevant.

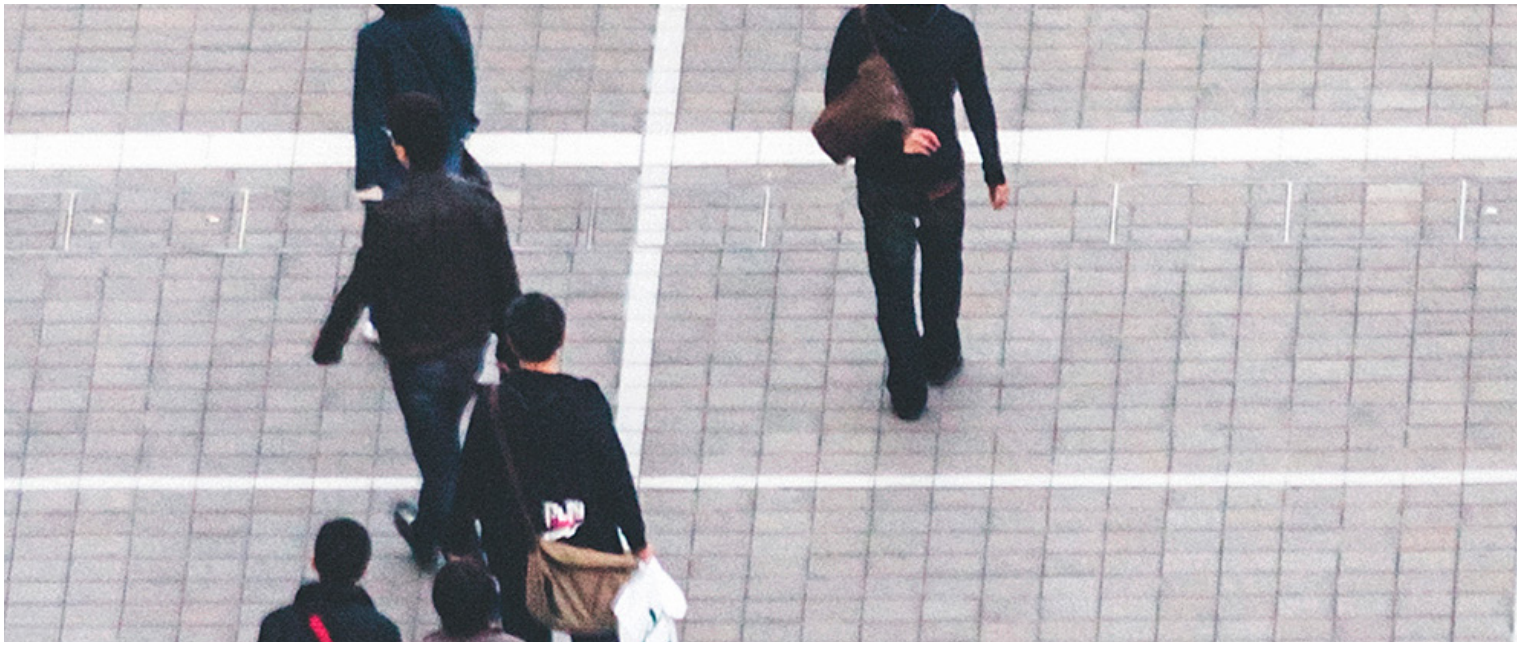
Restrictions on social media platforms have engendered lawsuits in various states challenging their constitutionality and based primarily on alleged First Amendment violations. Indeed, there is currently litigation in Tennessee and Georgia challenging the above statutes. Federal courts in Ohio and Arkansas have also recently struck down similar social media statutes in those states. It is unknown whether Virginia's law will suffer a similar fate or face such challenges, but such efforts will likely not materialize, if at all, until after the statutory effective date of January 1, 2026.

Virginia implications for social media platforms

Social media platforms have until January 1, 2026, to update their services to adhere to Virginia's newly restrictive law. Platforms must develop 'commercially reasonable methods,' such as neutral age screen mechanisms, to help identify users under the age of 16, and then set default time limits of one hour per day for those qualifying minors. Beyond that, platforms will need to deploy new technologies that allow parents or legal guardians of minor users to provide 'verifiable consent' to adjust the allotted time limits for their children. Given the statute's delineated exceptions that exclude application in many instances, companies that believe they may be impacted should consult knowledgeable external legal counsel to ensure that the law applies to their business. For covered companies under the law, legal counsel can also advise whether deployed technologies comply with the law's mandates.

Virginia's action adds to an overall regulatory scheme that is increasing in complexity. As noted above, state laws addressing social media vary in scope and substance. Companies must be prepared to navigate this ever-expanding patchwork of laws to avoid incurring steep monetary penalties, injunctive measures, and reputational damage. Those platforms operating on a national scale may want to adopt measures that satisfy the most restrictive state law requirements to ensure they remain in compliance within each state.

Virginia's recent enactment, within a state that is traditionally business-friendly, should signal to companies that state governments across the political spectrum are deeply concerned with protecting children on social media platforms. Other states will undoubtedly consider similar laws in the coming months and years. Affected businesses should continue to monitor related legislation and be prepared to adjust their business models and practices accordingly to mitigate regulatory risk.



Country Profile: Philippines

Legal frameworks on data privacy and AI systems processing personal information in the Phillippines

Edsel F. Tupaz
Senior Partner
aeftupaz@gorricetalaw.com
Gorriceta Africa Cauton & Saaavedra, Philippines

Acknowledgment: Special thanks to Gabriel T. Tabeta, Angela T. Mercado, and Julia S. Unarce, Associates at Gorriceta Africa Cauton & Saavedra, for their valuable research and contributions to this article.

Introduction

The Philippines has long recognized the constitutional right to privacy, but the enactment of the Data Privacy Act of 2012 (the Act) marked a significant leap toward a comprehensive regulatory framework aligned with international standards. With the National Privacy Commission (NPC) at the helm, the country continues to develop its data protection regime following leading use cases that affect Philippine data subjects, underscoring the Act's relevance in today's digital landscape in the Philippines.

The Philippine Act

Amid increasing digitization and rapidly emerging digital economies, the Act was enacted in 2012 to strengthen the protection of personal information in the country. It is one of Asia's earliest comprehensive statutes on personal data privacy, with origins tracing from the Asia-Pacific Economic Cooperation (APEC) Privacy Framework and the European Union (EU) Data Protection Directive of 1995.
The Act created a specialized government agency, the NPC, tasked with overseeing and ensuring compliance with the Act. The NPC has the power to issue, revise, and enforce rules and regulations, investigate complaints, adjudicate data privacy violations, and monitor compliance. When violations are found, the NPC may impose fines and other penalties, as well as civil damages, under the Act, its Implementing Rules and Regulations (IRR), and relevant issuances.

Material and territorial scope of the Act

The Act applies only to the processing of personal data, categorized into three types:

- personal information or data from which the identity of an individual is apparent, or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual;
- sensitive personal information or data:
  - relating to an individual's race, ethnic origin, marital status, age, color, and religious, philosophical, or political affiliations;
  - relating to an individual's health, education, genetic, or sexual life, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
  - issued by government agencies and peculiar to an individual, which includes, but is not limited to, social security numbers, previous or current health records, licenses or their denial, suspension, or revocation, and tax returns; and
  - specifically established by a Philippine executive order or an

act of the Philippine Congress to be kept classified; and
- privileged personal information or data considered privileged communication under the Rules of Court or other laws, such as those protected by attorney-client confidentiality.

Certain processing activities relating to government officials, journalism, research, law enforcement, and personal data originally collected from residents of foreign jurisdictions are exempt from the scope of the Act.
In terms of its territorial scope, the Act applies to personal information controllers (PICs) and personal information processors (PIPs) outside of the Philippines when such entities process personal data of Philippine citizens or residents, or when the PIC or PIP has links with the Philippines.

General personal data processing principles under the Act

Under the Act, the processing of personal data must adhere to the following principles.

1. Transparency

PICs and PIPs must process personal data only for specified and legitimate purposes that are clearly communicated to data subjects at or before the time of collection.

The transparency principle is best elaborated in the NPC Guidelines on Consent, which require PICs to ensure that data subjects are informed of the nature, purpose, and extent of the processing. These disclosures must include the identity of the PIC, applicable risks and safeguards, the rights of the data subject, and how those rights can be exercised. Information should be provided at the time consent is obtained, with further details accessible through a layered privacy notice (e.g., hyperlinks to comprehensive policies). Clear, plain, and accessible language must be used, and PICs must avoid vague terms, technical jargon, or confusing phrasing. All information must be easy to access and presented in a manner that an average member of the target audience can understand.

The NPC Guidelines on Child-Oriented Transparency contextualize the transparency principle to the unique needs of children. PICs must ensure that children understand the nature, purpose, and extent of data processing. Privacy notices must be tailored to children's best interests and evolving capacities, with PICs encouraged to use age-appropriate formats to ensure readability, comprehension, and clarity. Before offering services or products likely to be accessed by children, PICs must conduct child Privacy Impact Assessments (PIAs) to evaluate risks specific to children. Based on the results, PICs and PIPs must implement appropriate safeguards, including age-assurance mechanisms to estimate the age range of users, and adjust privacy measures accordingly.

2. Proportionality

PICs are only allowed to process such amount and kind of personal data that is adequate, relevant, suitable, necessary, and not excessive in relation to its stated purpose. Further, PICs are only allowed to process personal data when the intended purpose cannot be reasonably achieved through less intrusive means. In cases where personal data is disclosed to third parties, data disclosures must be limited to their declared, specified, and legitimate purpose.

In one instance, the NPC ruled that recording phone calls for recordkeeping and to use in future legal disputes was disproportionate, as the PIC failed to show that these objectives could not be met through less intrusive means - see the NPC Advisory Opinion No. 2023-010 re: Recording of Telephone Conversation Through Voice Over Internet Protocol (VoIP).

3. Legitimate purpose

The PIC's processing of personal information must be compatible with a declared and specified purpose that is not contrary to law, morals, or public policy. The processing of personal data may only be done when the PIC or PIP has a lawful basis for processing.

Processing personal information is allowed when:
- the data subject has given their consent;
- the processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;
- the processing is necessary for compliance with a legal obligation to which the PIC is subject;
- the processing is necessary to protect vitally important interests of the data subject, including life and health;
- the processing is necessary to respond to a national emergency, to comply with the requirements of public order and safety, or to fulfill functions of a public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or
- the processing is necessary for the purposes of the legitimate interests pursued by the PIC or by a third party or parties to whom the data is disclosed, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

Out of these grounds, consent and legitimate interest are most invoked by PICs. Hence, the NPC subsequently issued circulars, including the Guidelines on Legitimate Interest, clarifying the proper application of these lawful bases for further guidance.

On the other hand, processing privileged personal information and sensitive personal information are prohibited and are allowed

only under exceptional circumstances involving the data subject's consent, a law authorizing such processing, in cases necessary to protect a person's life or health, or if necessary to protect certain legal rights and interest in court proceedings.

A recent NPC Advisory Opinion (No. 2023-001, re: Disclosure of Unit Owners' Personal Data and Related Documents) clarified that processing based on a claim of a legal right, interest, or defense does not require an ongoing proceeding before any administrative, judicial, or quasi-judicial body, nor must it result in the initiation of a formal case.

Data subject rights

Under the Act, data subjects have the following enforceable rights against PICs (and, in some cases, against PIPs), who, in turn, must comply when such rights are invoked without undue delay and within 30 working days.

- Right to be informed: Data subjects must be informed if their personal data will be or has been processed, along with their rights and information on the nature, purpose, and methodologies of processing, including the existence of automated decision-making and profiling, prior to or at the next practical opportunity after processing.
- Right to access: Data subjects may confirm the existence of any processing activity and obtain information on how and when their personal information was processed, its sources, recipients, and the reasons for disclosure.
- Right to object: If the processing is based on consent or legitimate interest, data subjects may object to the processing of their personal data, and if there are significant changes or amendments to a consent form, they must be notified and given the right to object and/or withdraw previously given consent.
- Right to rectification: Data subjects may dispute and correct inaccuracies or errors in their personal data within a reasonable period of time.
- Right to erasure or blocking: Data subjects may request the suspension, withdrawal, blocking, removal, or destruction of personal data from the PIC's filing system, in both live and backup systems, when there is substantial proof of any of the grounds to do so.
- Right to data portability: In cases where the processing is based on consent or a contract, the data subject may obtain from the PIC a copy of the personal data and, when the personal data is processed by electronic means and in a structured and commonly used format, have the same transmitted from the PIC to another.
- Right to file a complaint and to damages: Data subjects may file a complaint in case of misuse, malicious disclosure, and any other violation of the Act. The NPC may impose civil damages, fines, and other administrative sanctions, and forward the complaint to the Philippine Department of Justice for the filing of a criminal case, if necessary.

Deceptive design patterns

The NPC clarified in its Guidelines on Deceptive Design Patterns that using deceptive design patterns in personal data processing constitutes deception and coercion, which can invalidate a data subject's consent. Accordingly, PICs must avoid such practices to uphold the principle of transparency.

Cross-border transfers of personal data

In its Advisory No. 2024-01 on Model Contractual Clauses for Cross-Border Transfers of Personal Data, the NPC prescribes the use of Model Contractual Clauses (MCCs) as a common mechanism in binding legal agreements for cross-border personal data transfers. While adoption is not mandatory, MCCs help PICs demonstrate accountability in such transfers by embedding data privacy safeguards in such agreements.

General obligations of PICs and PIPs in relation to the security of personal data in the Government and the private sector

NPC Circular No. 2023-06, entitled Security of Personal Data in the Government and the Private Sector, recently took effect. This is considered the latest comprehensive update on all general requirements for the security of personal data processed by a PIC or PIP in the public and private sectors. Due to the general nature of this Circular, a PIC or PIP may implement more detailed or stricter policies and procedures that reflect industry-specific operating requirements. The Circular sets forth updated general obligations of PICs and PIPs to achieve compliance with the Act in terms of security measures, which include:

- designating a data protection officer (DPO) and registration of the PIC's or PIP's data processing systems;
- creating an inventory of data processing systems and activities;
- conducting and updating existing PIAs;
- setting an organization's privacy management program;
- periodically training employees, agents, personnel, or representatives on privacy and data protection policies; and
- complying with the NPC's orders when the PIC and PIP privacy and data protection policies are subject to review and assessment.

Several other rules and concepts are reiterated or underscored in this Circular and pertain to Privacy by Design and Privacy by Default principles, conducting a PIA on off-the-shelf software, solutions, or data processing systems, privacy engineering, particular requirements for storage, mandatory policies such as an acceptable use policy, secure authentication mechanisms, business continuity management and adopting a business continuity plan, telecommuting policies, requirements for emails and personal productivity software, removable or portable storage media, guidelines for disposal and destruction of personal data, and requirements for a personal data disposal service provider. Miscellaneous provisions include threat monitoring and vulnerability management, audit, and penalties.

Legal framework for data processing activities of AI systems

The Philippines currently lacks a dedicated artificial intelligence (AI) law, whether special or comprehensive. Nonetheless, AI use and its outputs remain subject to general laws, notably the Act, when personal data processing is involved.

Automated processing and profiling systems under the Act

The NPC defines automated processing as a series of processing operations performed on personal data where there is limited to no human intervention. This includes profiling or any form of automated processing using personal data to evaluate personal aspects relating to a natural person to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

The Act requires PICs to provide data subjects with access to information on automated processing whose outputs become the sole basis for making decisions that significantly affect them, and mandates obtaining consent for profiling or similar processes producing significant effects. PICs must also notify the NPC by registering automated processing and profiling systems with the NPC Registration System.

NPC Advisory No. 2024-04

NPC Advisory No. 2024-04 (the AI Advisory) requires AI developers and deployers to comply with the Act's principles, including the disclosure of AI processing purposes, inputs, and risks. PICs remain responsible for AI outcomes, even when data is transferred to third parties, and are required to implement documented governance and compliance measures, including:

- PIAs;
- Privacy by Design and Privacy by Default;
- industry-standard security;
- continuous AI monitoring;
- AI ethics boards;
- regular AI retraining and data scrubbing; and
- human oversight mechanisms.

Bias must be limited and manipulative AI practices must be prohibited, including AI washing. Data subjects must be able to exercise their rights meaningfully, including human review requests, without unreasonable refusal, and PICs must implement effective mechanisms or alternatives to uphold these rights even when direct enforcement is challenging in AI systems.

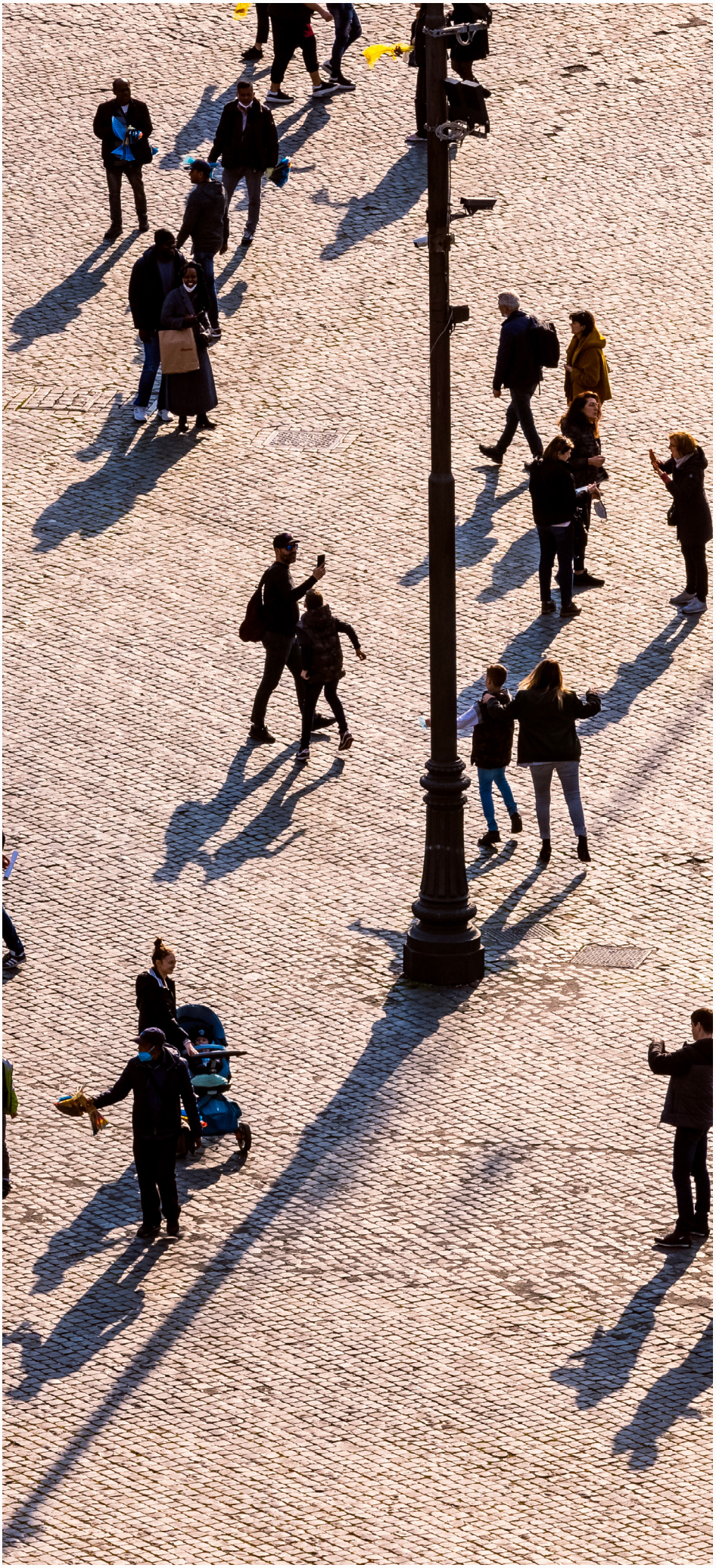
Relevant NPC advisory opinions on AI and data scraping

Prior to the AI Advisory, the NPC has confirmed that AI systems must comply with the Act regardless of processing methods, with PIC accountability for AI outputs. Use of legitimate interest as a lawful basis is allowed for employee performance scoring via AI only when decisions are not solely based on automated outputs; otherwise, consent is required. The NPC also stresses proportionality in data collection, and less intrusive alternatives should be prioritized, as exemplified by its rejection of SMS data use for credit scoring due to disproportionality.

Conclusion and ways forward for Philippine privacy compliance

The Philippines is seeing increased regulatory scrutiny over personal data processing. In 2022, two bills were filed in Congress seeking to amend the Act. House Bill No. 892 proposes harsher penalties and disqualification of public officials who violate the Act, while House Bill No. 898 seeks to redefine sensitive personal information to include biometric and genetic data, clarify extraterritorial application, set the digital age of consent at 15, and allow local representatives to report data breaches on behalf of foreign controllers.

The country's data protection regime is also expected to evolve in response to the expanding data needs of the digital and AI industries. Companies entering the Philippine market should treat data protection and data subject rights as baseline compliance requirements, not optional extras. Embedding Privacy by Design, adopting Privacy by Default, and implementing a comprehensive privacy management program are key compliance strategies. While there is no dedicated AI law yet, the NPC actively regulates data processing in AI development and deployment. Businesses must closely follow NPC advisories to ensure responsible AI use, build consumer trust, and maintain regulatory alignment, especially amid rising enforcement efforts and the public's strong adoption of emerging technologies.



Data transfers, their implications, and recent fines for social media companies in China

Dehao Zhang
Of Counsel
dehao.zhang@fieldfisher.com
Fieldfisher China, Beijing

China's data transfer practice is not a new topic, but many companies still feel unfamiliar, especially with the Regulations on Promoting and Regulating Cross-Border Data Flows adopted by the Cyberspace Administration of China (CAC). After a large technology and social media company was fined in the EU due to data transfers from the EU to China, some companies also worry about whether China will take enforcement action against the non-compliant companies. We will discuss China's personal data transfer requirements and particular requirements for transfers from the EU to China.

Personal data transfers outside of China

Personal Information Protection Law

Article 38 of the Personal Information Protection Law (PIPL) requires that where the business needs of a 'personal information handler' require the transfer of personal information outside of China, it should meet one of the following conditions:

- conduct a security assessment, which is organized by the CAC;
- get a certification that is in accordance with the CAC rules;
- use Standard Contract Clauses (SCCs) which have been published by the CAC; or
- follow other rules required by the CAC or other legal requirements required by other laws or regulations.

The PIPL also states that 'if the international treaties or agreements concluded or participated in by the People's Republic of China have provisions on the conditions for transferring personal information outside the territory of the People's Republic of China, the transfers can be implemented in accordance with such provisions. Personal information handlers shall take necessary measures to ensure that the processing of personal information by overseas recipients meets the personal information protection standards stipulated in this Law (namely the PIPL).'

Article 39 of the PIPL requires that 'if a personal information handler transfers personal information outside of the People's Republic of China, it shall inform the individual(s) of the name of the overseas recipient, contact details, processing purposes, processing methods, type of personal information, and the method and procedure for exercising the rights under the PIPL to the overseas recipient, and obtain the individual's separate consent.'

The PIPL requires that data transfers from China to other countries or regions must comply with the data transfer mechanisms under Article 38 of the PIPL. There are four different approaches for different types of companies/transfers. Additionally, the PIPL includes a transparency requirement noting that data subjects must be informed of certain information about the data importer.

Regulations on Promoting and Regulating Cross-Border Data Flows (the CAC Regulations)

Regarding the details of Article 38 of the PIPL, the CAC adopted the CAC Regulations to clarify how to enforce the legal requirements from the regulator's side. The CAC provided some useful exemptions for data transfer obligations (namely data transfer security assessments, SCCs, or certification) if the personal information handler's transfers meet one of the following:

- if data is not specifically notified or publicly released as important data by relevant competent authorities, data controllers do not need to conduct a data transfer security assessment for such data transfers;
- if data to be transferred does not contain any personal information nor important data;
- if data to be transferred is collected from other countries or regions but transferred to China, and the controller in China doesn't conduct any other processing but just transfers it outside of China;
- if the data transfer is necessary for the performance of a contractual obligation with data subjects;
- if the data transfer is necessary for the performance of internal HR rules for global HR management purposes;
- if the data transfer is necessary for the protection of a natural person's life, health, and property safety; or
- if the number of data subjects involved in the transfers is fewer than 100,000 per year, when there is no sensitive data to be transferred, and if the data exporter is not a critical information infrastructure operator (CIIO).

If the exemptions above cannot be relied on by the controller who is an exporter, the controller shall analyze which mechanism they can use. The exporter/controller cannot freely choose the mechanisms as different mechanisms apply to different transfers according to different thresholds. These thresholds are as follows:

Categories	CAC security assessment	China SCCs filing work	Certification
Important data transfers	If a controller transfers important data outside of China	/	/
CIIO's personal information transfers (if the transfers do not fall under exemptions)	If a CIIO is a controller whose transfers do not fall under any exemptions, it should conduct the CAC's security assessment	/	/
Non-CIIO's personal information transfers (assuming there is no sensitive data to be transferred, and if the transfers do not fall under exemptions)	If the controller is not a CIIO and transfers more than one million data subjects' personal information (without sensitive data) outside of China since January 1, 2025, it should conduct the CAC's security assessment	If a controller is not a CIIO and transfers more than 100,000 data subjects' personal information (without sensitive data) outside of China since January 1, 2025, it should use the China SCCs	Recommended rather than mandatory
Non-CIIO's personal information transfers (assuming there is sensitive data to be transferred and if the transfers do not fall under exemptions)	If a controller is not a CIIO and transfers more than 10,000 data subjects' sensitive data outside of China since January 1, 2025, it should conduct the CAC's security assessment	If a controller is not a CIIO and transfers fewer than 10,000 data subjects' sensitive data outside of China since January 1, 2025, it should use the China SCCs	Recommended rather than mandatory

Network data security management

There were also changes after the Regulations on Network Data Security Management (the Regulations) became effective on January 1, 2025. Article 35 of the Regulations states that 'if one of the following conditions is met, a network data handler can transfer personal information outside of China:'

- if the handler passes the data transfer security assessment organized by the CAC;
- if the handler obtains a personal information protection certification by professional institutions in accordance with CAC Regulations;
- if the handler complies with the provisions of the SCCs on the transfer of personal information formulated by the CAC;
- if the transfer of personal information outside of China is necessary to conclude and perform a contract with an individual as a party;
- if the transfer of employees' personal information outside of China is necessary to implement cross-border HR management in accordance with the labor rules and regulations formulated according to laws, and/or collective contracts signed according to laws;
- if the data transfer is necessary to fulfill statutory duties or obligations;
- if the data transfer is necessary in case of an emergency in order to protect the life, health, and property safety of natural persons; or
- if other conditions apply, which are stipulated by laws, administrative regulations, or rules of the CAC.

The requirements are similar under the PIPL and the Regulations, but these Regulations clarify that transfers necessary for statutory duties or obligations may take place. This differs from previous requirements and is helpful for organizations.

Negative list of data transfers adopted by the pilot free trade zones

The CAC Regulations stipulate that pilot free trade zones can independently develop a negative list of data exports within the framework of the national data classification and grading protection system. Data transfers covered by the list will be required to use data transfer mechanisms according to Article 38 of the PIPL. After approval by the provincial network security and information technology committee and filing with the CAC, data transfers outside the negative list will be exempt from applying for security assessments, entering into standard contracts, and passing protection certifications. This is an innovative measure to promote and facilitate cross-border data flow in pilot free trade zones.

Currently, Tianjin, Beijing, Hainan, Shanghai, Zhejiang, and other pilot free trade zones, ports, have adopted negative lists for data transfers outside of China, covering 17 fields including automobiles, pharmaceuticals, retail, civil aviation, reinsurance, deep-sea industries, and seed industries, and the CAC is guiding more free trade zones to develop negative lists for data exports.

Cases of data transfers

There are no administrative enforcement cases/fines related to non-compliance with the data transfer mechanisms (security assessments, SCCs, certification, or the CAC's rules), but there is a court case related to transparency and consent requirements of data transfers, which is required by Article 39 of the PIPL. In this case, the court held that if the hotel (namely, the exporter) transfers personal information outside of China to the EU and other countries, it should update its privacy policy to contain the requirement of Article 39 of the PIPL. However, the hotel failed to do so before transferring data, arguing that transferring personal information is necessary for performing contractual obligations with individuals. The court reviewed the evidence, including the hotel's privacy policy, and held that the hotel's purpose for transfers includes direct marketing and experience-enhancing purposes, which should not be necessary for performing contractual obligations with individuals. Therefore, such processing should be based on the legal grounds of consent, and, in this case, for transfers outside of China, the consent should be stand-alone consent rather than general consent.

This case becomes a useful training course for companies, especially international companies with subsidiaries and businesses in China, as normally such companies draft their privacy policies based on the EU's GDPR and California's CCPA, rather than China's PIPL. However, this case shows that there are gaps between the GDPR and PIPL requirements, and that privacy policies should be reviewed based on this.

Similarly, some international companies have been fined by South Korea's Personal Information Protection Commission due to the transparency requirement of data transfers.

EU data transfers to China and its implications

This is a big topic, especially as the EU does not have an adequacy decision with China on data protection. This means that companies' transfers have to rely more on EU SCCs.

However, after the Schrems II case, transferring data from the EU to China is more complicated given the national security where the importer is located and the possibility that law enforcement authorities may require the data importer to disclose EU personal data. Therefore, EU SCCs may be rendered an invalid mechanism for legally transferring personal data from the EU, as some countries' legislation may require actions that would not comply with the obligations of the EU SCCs.

Despite this, the EU SCCs have been updated, and Transfer Impact Assessments (TIA) are used to assess whether the data importer can create a level of data protection similar to the EU's GDPR and block access from authorities of the other country. However, this is still a complex topic as China has many laws that grant access rights to governmental authorities to data retained in China (no matter whether it concerns Chinese data or EU data), and EU regulators do not view this as safe or compliant with the GDPR.

A social media company's transfer of data from the EU to China resulted in a fine from an EU Member State's regulator, further emphasizing this complicated area of data protection. Some of the reasons for the fine given by the regulator include the fact that the Chinese national security-related legislation listed by the EU regulator grants Chinese governmental agents rights to access the data from the EU. However, the Chinese Government must still comply with China's PIPL and Data Security Law, which means the Government still needs to limit its access to only the scope necessary. This is a misunderstanding that the laws will give the Government unlimited rights to access EU data. Additionally, the company chose to rely on EU SCCs to protect the EU personal data at a GDPR level, as there is no adequacy decision between the EU and China. If the EU courts or regulators believe that China's legislation does not provide a sufficient level of protection for data, it may be necessary to look at how the company implemented the SCC obligations.

This case challenges Chinese companies that have businesses in the EU as they could face similar situations. The GDPR also considers remote access to be data transfers, but this still presents a lower risk than directly storing EU data in China, as only remote access on the systems without download would block EU data from Chinese governmental agents' access. In most cases, the governmental agents do not have the right or law enforcement capability to access a system based outside of China, especially if there is no Chinese data in such system. However, companies must consider the heavy financial cost and group management requirements involved.

If the EU and China were to negotiate an adequacy decision, this would change the situation and make data transfers between the EU and China more efficient.

DataGuidance

Interested in becoming a 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. Industry experts around the world partner with DataGuidance because we are committed to and invested in their success.

Industry expertise

- Recognition alongside global privacy professionals via our Experts Directory
- Over 20 years' working with Contributors across 300 jurisdictions
- Market leader in regulatory intelligence

Thought leadership

- Recognized thought leaders in privacy, security and AI governance
- Experts in over 300 jurisdictions

No financial ties

- No financial obligations for partnering
- Exclusive discounts to OneTrust DataGuidance

Our investment in your success

Global audience

- Over 2000 multinational organisations and 1600 customers
- Global customer base across numerous sectors and industries
- Regular promotion across social platforms to a wide audience

Critical compliance topics

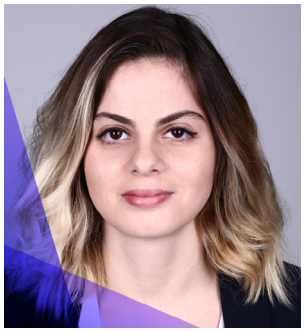
- Key privacy and security and AI areas covered
- Ever-growing and changing product to adapt to market need

Support

- Personalised content marketing support to facilitate accessibility and recognition
- Dedicated relationship management team and representative support
- Certain content eligible for 2-3 IAPP CPE credits
- Ongoing partner collaboration & resources

For more information please contact **contribute@onetrust.com**

Turkey cyberlaw - Key compliance requirements and challenges



Melike Hamzaoğlu
Partner
melike.hamzaoglu@hhklegal.com
Hamzaoğlu & Partners, Istanbul

Yücel Hamzaoğlu
Partner
yucel.hamzaoglu@hhklegal.com
Hamzaoğlu & Partners, Istanbul

Batu Kınıkoğlu
Partner
batu.kınıkoglu@hhklegal.com
Hamzaoğlu & Partners, Istanbul

Introduction: A new era in cybersecurity in Turkey

The growing reliance on digital technologies has rendered cybersecurity a fundamental element of national security policy. In light of evolving threats and the strategic importance of cyberspace, the Republic of Turkey has introduced a legal and institutional framework to enhance its cybersecurity posture.

On January 8, 2025, the Cybersecurity Directorate (the Directorate) was established by Presidential Decree with a mandate to formulate national policies and strategies, coordinate relevant stakeholders, and carry out awareness-raising and legislative activities. Subsequently, Cybersecurity Law No. 7545 (the Law) was adopted by the Grand National Assembly on January 15, 2025.

Although various sector-specific regulations had previously addressed aspects of cybersecurity, this Law represents the first comprehensive legislative initiative in Turkey that directly regulates cybersecurity as a standalone domain. Its enactment represents a significant milestone in formalizing the country's approach to digital risk management and national cyber resilience.

The scope of the Law encompasses public institutions and organizations, professional bodies with the status of public institutions, natural and legal persons, and organizations without legal personality that are present in cyberspace, carry out activities, or provide services. This wide-ranging scope underscores the Law's comprehensive reach, affecting virtually all actors engaged in digital environments, regardless of their legal status.

Within this framework, the Law introduces mandatory safeguards for critical infrastructure, imposes product-certification duties, and grants the State broad oversight powers over both public and private actors. Although these measures are intended to strengthen national resilience, they also give rise to potential issues, most notably definitional ambiguities, increased administrative burdens, and questions about proportionality.

Mandate, authority, and strategic framework of the Cybersecurity Directorate

The Directorate's mandate is broadly defined to cover cybersecurity activities across both regulatory and operational domains. The Directorate is responsible for:

- drafting national cybersecurity strategies and technical standards;
- ensuring coordination between public institutions and private sector stakeholders;
- maintaining an inventory of critical infrastructure information systems; and
- identifying and implementing the necessary security measures for their protection.

It also carries out testing and certification processes for cybersecurity products and services, mandates the use of certified and authorized solutions, and encourages the adoption of domestic technologies.

The Directorate is vested with audit powers, which may be exercised through both risk-based inspections and ad hoc reviews, the latter referring to unplanned, case-specific audits conducted outside the scheduled program when immediate attention is required, such as in response to emerging incidents or observed irregularities.

Where necessary, the Directorate may conduct on-site evaluations concerning any activities within the scope of the Law. Furthermore, the Directorate is authorized to conduct searches, as well as data copying and seizure procedures, in residences, workplaces, and non-public areas with a court order, or, in urgent cases, based on the written authorization of a public prosecutor. For authorized data center operators, such procedures can only be conducted with a court order. Notably, searches and seizures involving public institutions do not require a judge's order.

Strategic decision-making processes of the Directorate are guided by the Cybersecurity Council (the Council), which was also established under the Law. Chaired by the President, the Council comprises relevant ministers and high-level public officials. Its functions include approving national cybersecurity strategies, designating critical infrastructure sectors, and resolving disputes over competencies between public institutions. The implementation of Council decisions is overseen by the Directorate, ensuring a clear distribution of responsibilities between policy formulation and operational execution.

Key provisions introduced by the Law

The Law imposes a broad set of cybersecurity obligations on all entities that provide services and collect or process data through information systems, including both public institutions and private sector actors. Within this framework, relevant actors are required to promptly report any identified vulnerabilities or cyber incidents to the Directorate, provide all requested information, documents, hardware, and software in a timely and prioritized manner, and implement prescribed technical and administrative safeguards.

One of the most important provisions of the Law concerns the identification and protection of critical infrastructures. The Law defines critical infrastructure as information systems whose confidentiality, integrity, or availability, when compromised, may have serious consequences for national security, public order, or economic stability. These critical infrastructure sectors are designated by the Council; the identification of critical infrastructure, their inventory, and risk analysis are under the responsibility of the Directorate. The Directorate is also responsible for taking or requiring the implementation of security measures for critical infrastructure assets. As a result, organizations operating in sectors such as energy, banking, telecommunications, and public services will be subject to a range of obligations introduced by forthcoming secondary regulations, in addition to the sector-specific regulations already in force.

Additionally, the Law imposes an obligation on public institutions and entities designated as critical infrastructure to maintain a detailed inventory of all assets they possess, including data inventories. These entities are also required to conduct comprehensive risk analyses of their assets and implement appropriate security measures based on the criticality of each asset, or ensure that such measures are taken. Establishing an asset inventory, identifying risks, and implementing necessary protections are of vital importance not only for institutional compliance but also for individuals within these organizations who are tasked with such responsibilities. Under the Law, failure to fulfill these duties, particularly when it results in a data breach due to inadequate protection against cyberattacks on critical infrastructure, may lead to criminal liability, including imprisonment for a term of one to three years.

Another key obligation introduced by the Law is the mandatory certification of cybersecurity-related products. In particular, software, hardware, and services must be tested and certified either by the Directorate or by parties authorized by it. Only cybersecurity experts, producers, or companies that have been certified and authorized by the Directorate may supply such products to be used in public institutions and critical infrastructures. This certification obligation is likely to be interpreted broadly, covering a wide range of domestic and international vendors that support public services and critical infrastructure. However, the precise scope, particularly with respect to foreign suppliers and the evaluation criteria, will be clarified through upcoming secondary legislation.

Furthermore, cybersecurity companies subject to certification, authorization, or licensing procedures must obtain formal approval from the Directorate before initiating their operations. Companies are also required to comply with national

cybersecurity strategies, action plans, and other regulatory instruments issued by the Directorate, including those aimed at improving institutional cybersecurity maturity. In this regard, the regulation is expected to create significant compliance obligations and operational costs, especially for multinational tech companies and cloud-based service providers.

Another fundamental obligation under the Law is the mandatory reporting of cybersecurity incidents. Natural and legal persons are required to promptly notify the Directorate of any cybersecurity incidents identified within their areas of operation. Based on these notifications, the Directorate may initiate audits and, if necessary, carry out search, data copying, and seizure procedures with a court order, or, in urgent cases, with written authorization of a public prosecutor.

Legal ambiguities and challenges under the Cybersecurity Law

Certification requirements and market participation

The Law establishes a robust certification framework that governs the development, supply, and use of cybersecurity-related software, hardware, systems, and services. The Cybersecurity Directorate is responsible for overseeing the certification and testing of these technologies, including the creation and operation of dedicated testing infrastructures. In addition to evaluating technical products, the Directorate also manages the certification, authorization, and accreditation of cybersecurity companies and professionals, often in coordination with other relevant institutions.

Minimum security standards will be defined for cybersecurity solutions, and all related products will be subject to compliance assessments. The Directorate holds the authority to require necessary adjustments to ensure conformity with these standards. Where such requirements are not met, it may implement restrictive measures to prevent the use of non-compliant technologies.

Cybersecurity companies subject to certification, authorization, and licensing requirements must secure approval from the Directorate prior to launching their services. This framework applies broadly to domestic and international actors alike and is expected to significantly influence market dynamics, particularly for vendors supplying to public institutions and critical infrastructure sectors.

The certification and approval process is designed to promote trusted solutions, ensure resilience across digital infrastructure, and foster alignment with national cybersecurity priorities. However, it also imposes rigorous procedural requirements that may affect market entry, especially in the absence of clear, detailed secondary legislation. The resulting compliance burden may be particularly acute for smaller enterprises and foreign suppliers unfamiliar with local certification and approval pathways.

Export control and market access limitations

The export of cybersecurity-related products, systems, software, hardware, and services is subject to regulatory oversight by the Directorate. Such exports must comply with procedures and principles to be determined by the Directorate, and the export of specified items may only proceed upon obtaining prior approval. This approach is intended to ensure that sensitive digital technologies with potential national security implications are not transferred abroad without adequate scrutiny.

In addition to export controls, corporate transactions involving companies that develop or supply cybersecurity technologies, such as mergers, demergers, share transfers, or sales, must be reported to the Directorate. Transactions that result in direct or indirect control or decision-making authority over such companies, whether by a single party or jointly, are subject to prior authorization. This extends regulatory oversight to structural changes that may affect the integrity or ownership of cybersecurity assets.

While aligned with global efforts to safeguard national security and critical infrastructure, the implementation of these controls may create legal uncertainty in the absence of clear secondary regulations and interpretative guidance. Without defined criteria and procedures, stakeholders, especially in cross-border transactions, face ambiguity regarding authorization requirements. The Directorate is expected to issue secondary legislation in the near future to address these gaps.

Administrative powers and legal balance

The Law establishes broad administrative powers over digital infrastructure through institutions affiliated with the executive branch. Within this framework, the Directorate is authorized to request information and documents from all digital system users, not limited to public institutions. It may also conduct on-site inspections and enforce technical and administrative security measures where necessary. Although an earlier draft of the Law allowed the Directorate to copy and seize digital data without a court order, this provision was removed in response to public criticism.

Nevertheless, the final version of the Law continues to grant the Directorate substantial powers of oversight and intervention, particularly given that individuals or organizations subject to searches of their residences or workplaces, or the seizure of documents or devices, will not be notified prior to the execution of such actions. However, the actual scope and implementation of these powers will largely depend on forthcoming secondary regulations and how they are applied in practice.

Vague terminology and compliance risks

Several key concepts introduced under the Law, most notably 'critical infrastructure' and 'cyber threat intelligence,' are ambiguously defined, creating considerable interpretive uncertainty in both regulatory and compliance contexts. For instance, although the authority to designate critical infrastructure sectors is assigned to the Council, the Law provides no specific criteria, procedural safeguards, or avenues for appeal to guide or constrain this discretion. While it is expected that secondary legislation will address such gaps, the enabling provisions currently grant broad powers to regulatory authorities, raising concerns about inconsistent implementation and potential administrative overreach. It is anticipated that sectors such as energy, telecommunications, finance, and defense will be designated as part of the critical infrastructure sectors.

This ambiguity is also evident in the treatment of 'cyber threat intelligence.' Although the Law defines it as processed or enriched information regarding existing or potential cyber threats and attacks targeting assets in cyberspace, it fails to clarify the operational scope, permissible data sources, or acceptable analytical methods. The practical and legal consequences of these definitional gaps are significant. Where violations carry administrative or criminal penalties, the absence of clear definitions undermines the principles of legal certainty and proportionality.

Sanctions and legal consequences

The Law adopts a tiered sanction regime to ensure deterrence and compliance, distinguishing between criminal penalties and administrative fines based on the severity of the violation. While serious offenses such as unauthorized cyberattacks, data breaches involving personal or institutional information, and the unlawful dissemination of leaked data are subject to imprisonment ranging from one to 15 years, other types of misconduct, such as failure to implement required technical measures, obstructing inspections, or non-compliance with notification obligations, may result in substantial administrative fines. The monetary penalties stipulated under the Law range from TRY 100,000 to TRY 100 million (approx. $2,500 to $2.5 million), with certain violations subjecting companies to fines of up to 5% of their annual gross sales revenue. The following table presents the sanctions applicable under the Law:

Violation type	Type of sanction	Explanation
Failure to provide requested information, documents, data, software, or hardware to authorized institutions.	1-3 years of imprisonment and 500-1,500 days of judicial fine.	Obstruction of inspection processes by institutional or individual actors.
Unauthorized activity without obtaining required licenses or approvals.	2-4 years of imprisonment and 1,000-2,000 days of judicial fine.	Engaging in cybersecurity-related operations without legal authorization.
Breach of confidentiality obligations.	4-8 years of imprisonment.	Disclosure of information legally required to be kept confidential.
Unauthorized access, sharing, or sale of personal or institutional data.	3-5 years of imprisonment.	Making data publicly available without the consent of the concerned individual or institution.
Dissemination of false information to create public fear or target institutions.	2-5 years of imprisonment.	Publishing false cybersecurity-related content with intent to incite fear or defame entities.
Cyberattacks targeting Turkey's national digital infrastructure or storing any data obtained as a result of these attacks and kept in cyberspace.	8-12 years of imprisonment.	Attacking critical digital systems or storing data obtained through such attacks.
Dissemination, export, or sale of data obtained through cyberattacks.	10-15 years of imprisonment.	Transferring or making available data acquired from cyberattacks to third parties.
Abuse of duties and powers arising from the Law or failure to protect critical infrastructure resulting in data breach.	1-3 years of imprisonment.	Negligent or unlawful conduct by officials leading to data loss or exposure.
Failure to comply with technical duties such as use of certified products or mandatory notifications.	Administrative fine: TRY 1 million to 10 million (approx. $25,000 to $250,000).	Violation of prescribed technical or administrative security measures and failure to report cyber incidents.
Exporting cybersecurity products and engaging in corporate transactions, such as mergers and acquisitions, without compliance with regulatory requirements.	Administrative fine: TRY 10 million to 100 million (approx. $250,000 to $2.5 million).	Not following the rules when exporting cybersecurity products or doing corporate transactions.
Failure to cooperate with inspectors or obstructing audits.	Administrative fine: TRY 100,000 to 1 million (approx. $2,500 to $25,000).	Not following the rules when exporting cybersecurity products or doing corporate transactions.
For companies: up to 5% of annual gross sales revenue, not less than TRY 100,000 (approx. $2,500).	Non-compliance during official inspections; revenue-based penalties for corporations.	Non-compliance during official inspections; revenue-based penalties for corporations.

Implementation and transitional enforcement

The implementation of the Law is supported by transitional and institutional restructuring provisions designed to ensure a smooth transfer of responsibilities and regulatory continuity. Within six months of the Law's enactment, all assets, infrastructure, records, and liabilities related to national cybersecurity functions currently held by the Information and Communication Technologies Authority and the Digital Transformation Office will be transferred to the newly established Directorate.

Entities operating in the cybersecurity space, including associations, federations, foundations, and commercial companies, are required to complete certification, authorization, and accreditation procedures within one year from the entry into force of the secondary regulations. Although these secondary regulations have not yet been published, they are expected to be issued in the near future. Failure to comply will result in the loss of legal capacity to operate in the sector. Non-compliant associations, federations, and foundations may be subject to judicial dissolution, while companies must remove all references to cybersecurity from their corporate charters and initiate liquidation procedures where necessary.

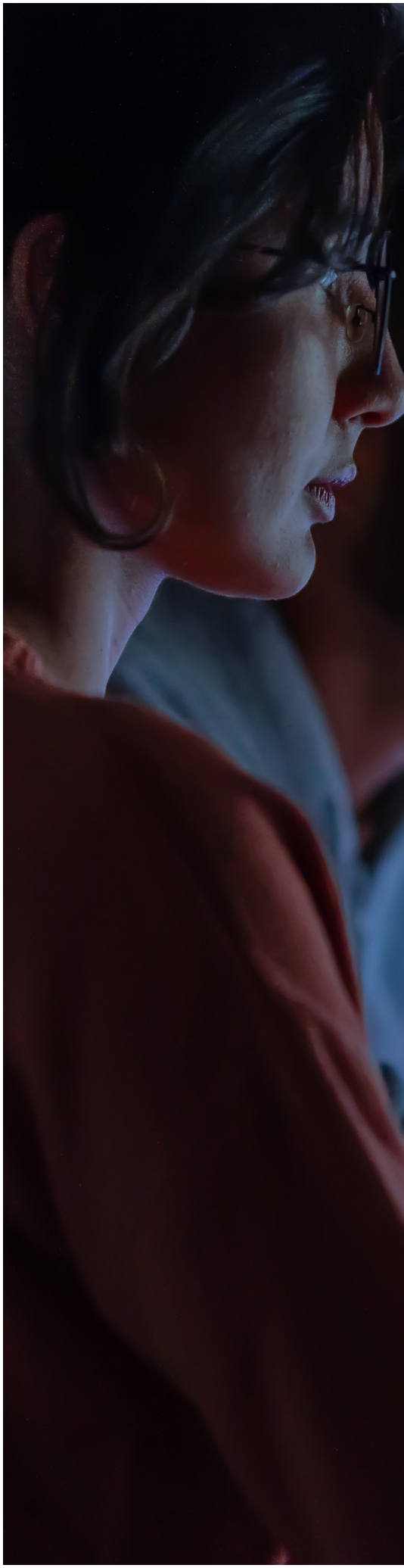
Until the institutional setup of the Directorate is fully completed, bodies operating under provisions repealed by the Law will continue their duties under existing rules. Secondary legislation required for the Law's implementation is to be issued within one year. In the interim, the existing regulations that do not conflict with the new Law will remain in force.

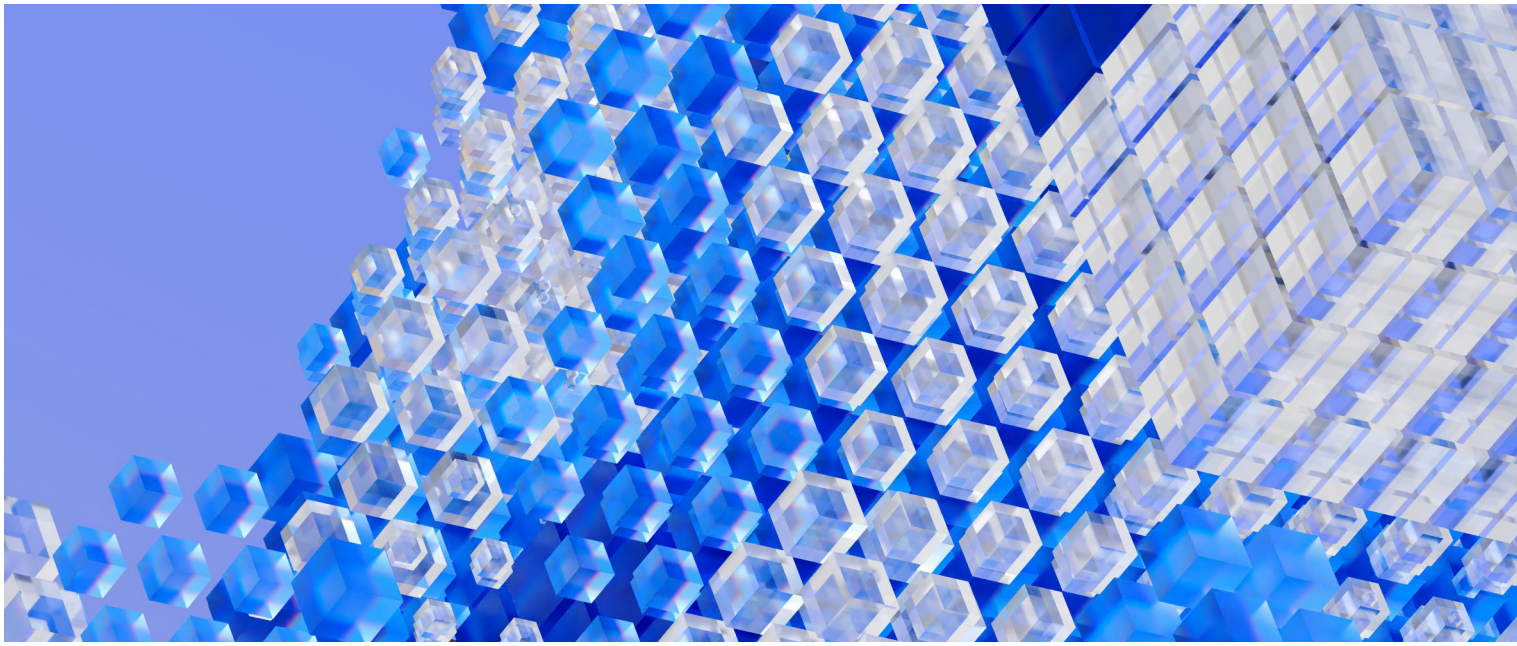
Conclusion

As discussed throughout this article, Turkey is undergoing a significant regulatory transformation in the field of cybersecurity. The new framework introduces extensive administrative powers, procedural mechanisms, and legal obligations that apply across both public and private sectors. The Law authorizes centralized oversight, mandates certification, and imposes specific obligations for the protection of critical infrastructure. Additionally, it requires critical infrastructure entities to maintain detailed asset and data inventories, conduct risk analyses, and implement appropriate safeguards. Failure to meet these obligations, especially if resulting in a data breach, may lead to criminal liability, including imprisonment. While these reforms aim to enhance national resilience in the digital domain, they also present notable compliance challenges.

Of particular concern are the ambiguities surrounding key legal terms, the broad scope of administrative discretion, and the possibility of overlapping regulatory obligations, especially in relation to data protection and competition law. The high financial and criminal sanctions, combined with tight audit and oversight mechanisms, may increase the legal and operational burden for both national and multinational entities operating in Turkey.

In light of these risks, the success of the cybersecurity reform agenda will ultimately depend on the clarity of secondary legislation, the consistency of administrative practice, and the establishment of a proportionate and transparent enforcement regime. Ensuring legal predictability while advancing national security interests remains a key challenge for Turkey's digital future.





Meet a DPO: Abel Kaszian

Abel Kaszian
Group Data Protection Officer
Abel.Kaszian@wizzair.com
Wizz Air, Budapest

Tell us about yourself and your role

I'm the Group Data Protection Officer (DPO) at Wizz Air. Think of me as the Luigi to Wizz Air's Mario – quietly making sure everything runs smoothly behind the scenes, dodging privacy Goombas and keeping our data castles secure. Jokes aside, my job is to ensure the privacy rights of flying customers (both in the air and on the ground), while also supporting the needs of a fast-growing business and the bells and whistles of the customer journey and engagement. This includes the usual DPO efforts and comes with all the challenges of being in such a role in 2025 – more on that below.

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

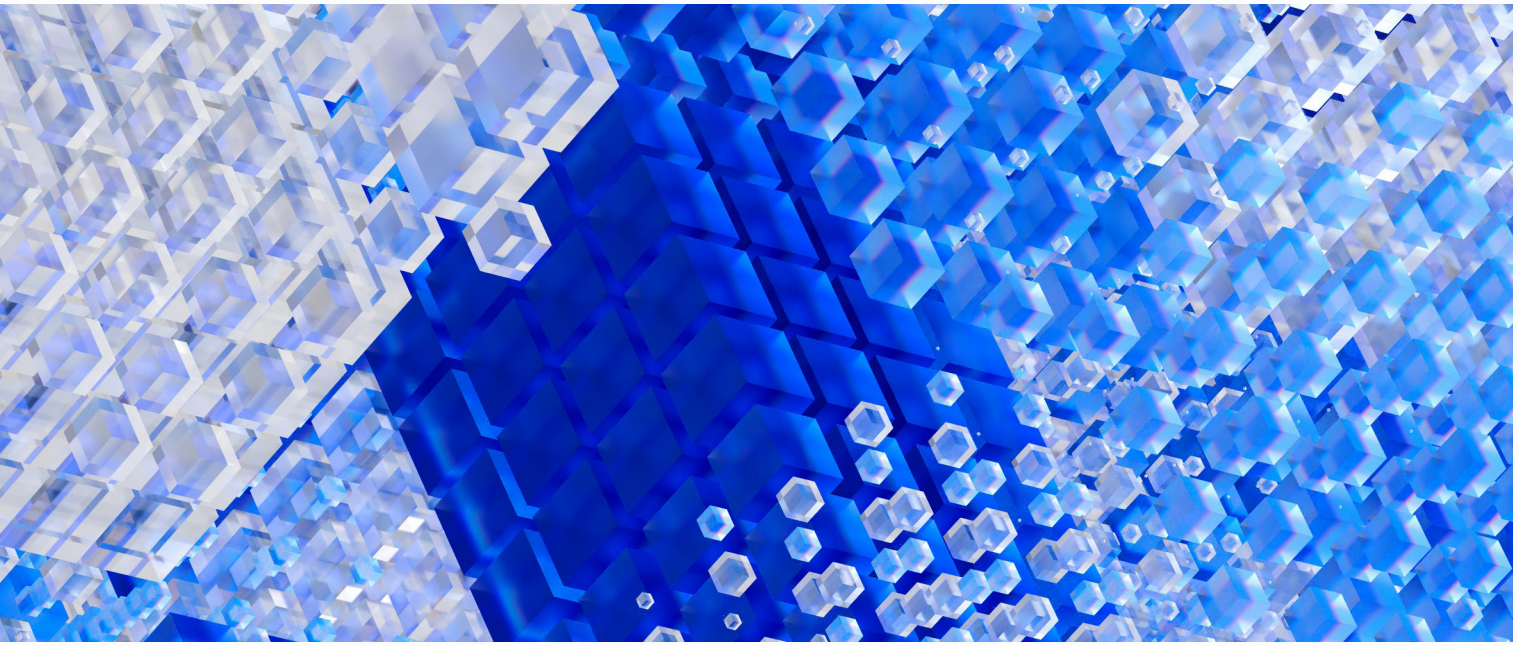
What I love is the need to connect with people. Personally, I think that the DPO role in 2025, if you want to be effective, is quite different from the independent advisor living in an ivory tower, as envisaged by the original text of the General Data Protection Regulation (GDPR). You actually have to be on the ground, working alongside business stakeholders, to understand their needs and collect sufficient resources for your privacy case. If you are not getting on well enough with business stakeholders and are a constant critic, you will basically suffocate yourself, and you won't have the necessary internal network or the detailed information needed for your privacy assessments. I always say that a 25-minute one-to-one coffee is worth 250 minutes of online meetings. After all, we are all individuals, humans, and data subjects at the same time.

The most challenging part is that the game never pauses. The rules keep changing, new regulations are introduced unexpectedly, and just when you think you've mastered one, another proposal is released. It is also generally challenging to strike the right balance between privacy rights and evolving technology. I sometimes wonder whether achieving complete privacy is even possible these days without significantly sacrificing one's quality of life, for example, by going totally off the grid and having no online presence whatsoever. However, I believe that, as privacy professionals, we can still ensure that personal data is only managed by one's own decisions, and that companies are transparent in general. This goes a long way with regulators as well.

What drew you to working in data protection and privacy?

Two things: One is a subject from my university years, which was taught by the deputy of the Hungarian DPA at the time. This was in the 17th century, of course, before the GDPR era. He made an analogy about privacy, saying that we should think about the things we do behind closed doors and curtains. Now imagine if that were not possible, and we had the feeling of constant surveillance and a lack of privacy.

This resonated deeply with me and is connected to the other deciding factor: My deep interest in technology and progress of the world in general. Year by year, privacy becomes more technology-focused, and it is unimaginable nowadays to think about this



topic independently of technology and its advances. My first experience of technology was playing Dune 2 on a 486 PC, and I have loved and been interested in technology ever since. This definitely helps me to understand current analytics and personalization tools, not to mention artificial intelligence (AI), and let's only mention it once in this article.

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

If I had to highlight one thing, it would be the never-ending debate about the GDPR: The constant criticism versus the support it receives. While we may disagree on the technical merits of the law, we must acknowledge its groundbreaking nature, despite its faults and quirks. It has changed the way we think about data protection worldwide, and many other countries have used the GDPR as a model for their own legislation.

Connected to this, I think the most complex compliance area nowadays is data transfers, not just between the EU and the US, but generally. As I have mentioned, I believe that, in the long term, we will need to adjust our perspective, as it is highly unlikely that a group of companies will be able to comply with all the intersecting rules, no matter how many Transfer Impact Assessments we prepare. We have to accept that there are different perspectives on data protection in different cultures, mixed with different technologies. In the era of constant internet connectivity and the Internet of Things, I am afraid it is impossible for anyone to be fully compliant. This is slightly concerning, but we must accept and adapt to the situation.

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?

Of course, the lightning-fast adoption of large language models (LLMs) and their insatiable appetite for data have raised long-standing questions about exercising privacy rights in these systems, which were previously unknown to at least 95% of privacy professionals four years ago. I am certainly an optimist, and I believe that it is possible to balance privacy rights with the data requirements of current technologies. However, I also believe that keeping personal data away from all online systems is an uphill battle. We must be realistic about our expectations and the changing world, and focus on transparency, explainability, and accountability.

What do you think the biggest challenge facing the data protection industry at the moment is? Will this change over the next five years?

The challenge lies in balancing innovation and protection. As technology evolves, systems are becoming increasingly complex, which makes it more difficult to build, read, and explain data flows. The industry also sometimes risks losing focus. We must remember that our primary goal is to empower individuals to practice their privacy rights and support them in doing so. As privacy professionals, we should never forget that we are also data subjects. With regard to the aforementioned focus, I am not sure whether new laws and guidelines or lawsuits by NGOs always contribute to this layer of protection.

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

Firstly, be like Link and stay curious, exploring every corner of Hyrule. Privacy law is constantly changing, so keep learning and don't be afraid to ask questions.

Secondly, build your network. These days, there are countless forums and roundtables related to privacy, cybersecurity, and data governance in every major city and jurisdiction. As I've mentioned, it is essential to be a useful DPO in this ever-changing landscape. It is also important to gain experience by listening to others and learning about current trends. Otherwise, it's easy to get lost in the myriad new regulations and DPA guidelines. While it's great to be 100% compliant, it's sometimes just not realistic. If you want to work in this field long term, you have to be wise and use the Pareto principle. If you persevere for a few years, plenty of opportunities will arise.

5 minutes with... Marton Domokos

Marton Domokos
Partner
marton.domokos@cms-cmno.com
CMS, Budapest

Tell us a bit about your job role and how you have progressed in your career.

I had the opportunity to work for CMS over 20 years ago, so it might seem like I grew up here. I had the chance to do a deep dive into data protection matters alongside learning more traditional areas of an international law firm, such as banking, M&A, and real estate. After passing the bar exam, my focus clearly shifted to technology law, and given the current 'tsunami' of digital regulations in the EU, it looks like it will stay that way for quite a while - which, I must say, brings me great challenges (and hopefully some benefits for our clients and colleagues as well). I also had the opportunity to complete several extended secondments at various clients, sometimes as a member of a specialized data protection team, other times as part of the general legal department, and occasionally even as its head. I am based in Budapest, and I am also responsible for overseeing our data protection practice in the CEE region.

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

In my next life, I would love to open a kindergarten. The closest I have come to working in this industry so far was when I helped my children's kindergarten with preparing a Data Protection Impact Assessment (DPIA), Legitimate Interests Assessment, and privacy notice for the security cameras in the parking lot.

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

What I love most is the chance to get familiar with a technology's risk aspects and help address any arising questions (ideally) before that technology is even launched. Overall, it is about helping our clients solve problems in ways that also benefit the broader public (e.g., breach management, transparency). What I find challenging is having to explain to privacy or legal skeptics why I love my job.

Where is your favorite place on earth?

Professionally, in a certain Brussels venue every November. Personally, anywhere I can spend quality time with my family - even if that sometimes includes pulling out the laptop. (Perhaps the most unusual spot I have ever taken a conference call was at a skatepark, where no matter how I adjusted my camera, skateboarders kept flying by in the background, not to mention the distinctive sound of skateboards hitting the concrete - all while I was in the middle of solving a personal data breach.)

Who would play you in a film about your life?

Definitely Nicolas Cage – he is my favorite actor, and my friends regularly send me those infamous memes because of it. Movie trivia: He already played an NSA employee in the movie about Edward Snowden, so he would be perfect for the role of a regular privacy lawyer, too. Calm

and organized for the day-to-day work, with the occasional burst of legendary 'Cage rage' during a particularly tricky bad faith data subject access request (DSAR).

What is your favorite book?

I would mention Atlas Shrugged by Ayn Rand – it is a thought-provoking and controversial dystopian novel about what happens when intellectual workers go on strike. There aren't any privacy lawyers in the book, but it is a fun thought experiment to imagine what would happen in real life if they did go on strike. I also recently revisited William Gibson's Neuromancer - such a poetic sci-fi book on so many levels. When I first read it at 13, I had no idea I would eventually end up working on the legal side of the kinds of technologies it envisioned.

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

After a particularly challenging regulatory filing, my colleagues would probably quote Gandalf's famous line from The Lord of the Rings in Moria's mines as an answer for this question. However, my (more professional) advice to junior lawyers wanting to specialize in technology law is that it is also important to gain experience in other areas of law throughout their career. This helps build cross-functional thinking – even at the same time, I find it fascinating that nowadays we have graduates applying to join our firm who specialize exclusively in interpreting a single EU technology regulation, such as the Digital Services Act (DSA) or the Digital Markets Act (DMA). Beyond that, a global mindset is essential - understanding trends and the broader regulatory and enforcement climate across different countries and continents is key to providing risk-based, practical advice.

Who is your inspiration?

Fortunately, I get to work in a field that continuously inspires me throughout my career, starting with those senior colleagues who, early on, recognized that data protection is not just a geeky thing but an important way to help clients. Younger colleagues also inspire me who, with their 24/7 professional community presence, are often more up-to-date than I am on regulatory developments. I also have to mention those clients for whom data protection is not just a minimal compliance burden but an area where they shape their company's practices, constantly inspiring me by showing that there is a genuine demand for the work we do. I am also inspired by and look up to those non-profit organizations that carry out important and sensitive societal roles, whom we support with pro bono privacy advice. For example, for children, the Bátor Tábor Foundation, the 'camp of courage,' or the Világszép Foundation, which supports children in foster care.

onetrust
DataGuidance

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