Ideas shaping privacy, published by OneTrust DataGuidance®

V7, ISSUE 2

MARCH 2025

Data Protection Leader

BRIDGING THE DIGITAL REGULATORY DIVIDE

APAC DEVELOPMENTS

Discussing 2024 updates in China, Hong Kong, Macau, Thailand, and Vietnam

DATA PROTECTION AND AI COMPLIANCE PROGRAM

Exploring necessary steps to ensure an effective program

CHILE COUNTRY PROFILE

Highlighting recent developments in data privacy law

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.

Wim Nauwelaerts
Partner, Alston & Bird LLP

Wim is a Partner at Alston & Bird, based in Brussels, where he advises clients on all matters and aspects involving EU and international data protection, cybersecurity, and AI. At the forefront of privacy and cybersecurity, his specialty lies in guiding multinational companies through intricate GDPR compliance issues, including as regards the EU's digital laws. With experience spanning almost three decades, Wim has become a trusted partner in the tech-savvy legal space.

James Gong
Partner, Bird & Bird

James is based in Bird & Bird's Beijing/ Hong Kong office, leading a data protection and cybersecurity team. He possesses extensive expertise in cybersecurity and data protection, as well as regulatory and transactional matters within the TMT sector. James advises a diverse clientele, including both foreign and Chinese multinational companies across various industries. He excels in guiding clients through data compliance projects with multi-jurisdictional elements and resolving complex legal issues. As a member of IAPP, he holds CIPP/E, CIPP/US, and CIPM certifications. Additionally, he is an expert with the Big DataGroup of the TC260 and serves as an arbitrator at the Shanghai International Arbitration Centre.

Fengming Jin
Associate, Bird & Bird

Ming is an Associate in the data protection and cybersecurity team at Bird & Bird's Beijing office. She specializes in data privacy, cybersecurity, telecommunications and internet, and labor law. Ming has provided privacy and data protection services to numerous domestic and international companies across various sectors, including finance, consumer goods, healthcare, internet, energy, aviation, and connected vehicles. She has conducted cross-border data transfer security assessments and assisted clients in achieving compliance, performed data protection due diligence, drafted and revised corporate compliance policies and documents, helped clients evaluate and enhance their internal data compliance systems, and supported domestic companies with their international expansion efforts.

Wilfred Ng
Partner, Bird & Bird

Wilfred Ng is a Partner in Bird & Bird's Commercial Department based in Hong Kong. As a technology, media, telecoms, and data protection lawyer, Wilfred is experienced in advising on all aspects of commercial, transactional, and regulatory matters in the TMT space, including data privacy and cybersecurity. This includes negotiating and preparing complex and cross-border technology contracts, licensing and development arrangements, collaboration, integration and managed services agreements, as well as advising on industry-specific regulatory issues in the payment services and fintech sectors.

Hwee Yong Neo
Senior Managing Associate, Bird & Bird

Neo is a Technology, Media, and Telecoms Lawyer in Bird & Bird's Commercial Department in Hong Kong. He frequently advises international clients and conglomerates on various commercial, technology, telecoms, and data privacy related matters, including AI. Neo frequently advises international clients and conglomerates on various technology and telecoms related legal, transactional, and regulatory matters concerning different types of services, systems, and technologies. This includes advising clients on AI (including generative AI) and the various practical, legal, and regulatory matters surrounding the development, use, and implementation of AI.

©Sane Seven

Dr. Sachiko Scheuing
European Privacy Officer, Acxiom

Dr. Sachiko Scheuing is the author of How to Use Customer Data and the European Privacy & AI Governance Officer of Acxiom. She is serving her fourth term as the Co-Chairwoman of FEDMA and is active in several European and global privacy and marketing associations and think tanks. She was one of the founding members of the EU DPO association, CEDPO. Sachiko is passionate about empowering women and girls and is serving as the global co-chair of Acxiom's gender equity program, WomenLEAD. In 2020, Sachiko received the DataIQ Professor Derek Holder Lifetime Achievement Award. In 2024, she was recognized by Women in Data® as one of the 20 most influential women in Data and Tech.

Jaime Urzúa W.
Associate, Alessandri Abogados

Jaime joined Alessandri in 2019, focusing his practice on corporate matters as well as in technology and entertainment. He advises companies on the implementation of personal data protection and cybersecurity programs in the financial, insurance, health, retail, and technology industries, among others. He advises clients in risk assessments, developing new lines of businesses, and designing strategies to protect their technological assets. Jaime also works in mergers and acquisitions, and advises domestic and foreign clients in the drafting, review, and negotiation of agreements and contracts. He is dedicated to talent representation and has assisted various artists, producers, television channels, and cultural managers, in connection with the music, film, and television industry, focusing on licensing, endorsement, and copyright management.

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

Cover page: Brian Eden/Moment via Getty Images, Page 4: Steve Proehl/The Image Bankvia Getty Images, Pages 6-7: Abstract Aerial Art/DigitalVision via Getty Images, Page 9: zhen li/Moment via Getty Images, Pages 10-11: DKosig/iStock via Getty Images, Pages 16-17: Eugene Mymrin/Moment via Getty Images, Pages 20-21: Rosmarie Wirz/Moment via Getty Images, Pages 22-23: Ezra Bailey/The Image Bank via Getty Images, Pages 24-25: Crispin la valiente/Moment via Getty Images, Page 27: Tom Werner/Stone via Getty Images, Pages 28-29: Monty Rakusen/DigitalVision via Getty Images, Pages 30-31: CHUNYIP WONG/iStock via Getty Images, Page 31: wera Rodsawang/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

Published by OneTrust DataGuidance™

Editorial

Much of what is wrong with the world right now has to do with our inability to see beyond our own tribes' narrative. Digital regulation should be a tool for effective and beneficial innovation.

Editorial: Bridging the digital regulatory divide

To deregulate or not to deregulate, that is the question. Or at least, it appears to be a key question in today's turbulent world of geopolitical tensions, technological competition, and anti-institutional stances. Countries around the world are apprehensively watching each other, fearful that their attempts to tackle the potential risks of artificial intelligence (AI) and other transformational technologies might get in the way of much needed economic growth. The aggressive deregulatory approaches of the US Federal Government seem to be having a chilling worldwide effect. Even the most prolific and influential digital regulation machine on the planet, the European Union, appears a little hesitant at the moment.

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

However, that slight hesitation is unlikely to dampen the relentless efforts to ensure a high level of protection for individuals and fundamental rights. So whether we are talking about privacy, cybersecurity, content moderation, or AI, the legal frameworks regulating those issues are unlikely to disappear anytime soon. How, then, can we bridge the emerging digital regulatory divide in a way that aligns responsible regulatory policies with the quest for technological innovation?

The first step needs to be avoiding brain-freezing and debate-suppressing dogmatism. Much of what is wrong with the world right now has to do with our inability to see beyond our own tribes' narrative. Digital regulation should be a tool for effective and beneficial innovation. Dogmatic views against or in favor of digital regulation suffer from a lack of realism that is, at best, paralyzing and, quite often, destructive. Conversely, there are many examples where a pragmatic approach to regulation and its aims become truly enabling. The recent package of measures unveiled by the UK Information Commissioner's Office (ICO) to drive economic growth is a palpable example of that. From data essentials training and pragmatic AI guidance to privacy-friendly online advertising and international data transfers, the ICO is not short of constructive and realistic thinking. Those who think that the ICO is a softie should take comfort in the fact that the mighty European Data Protection Board has also managed to apply real-world thinking to their analysis of how to make AI development compatible with the General Data Protection Regulation.

Any calls for regulatory pragmatism should of course be reciprocated by proactive engagement with policymakers and regulators by industry. This much needed engagement must be underpinned by openness and aimed at educating those tasked with making regulatory decisions. Everyone involved in digital regulation has much to learn about the constantly evolving digital world. In the same way we learnt decades ago about how cookies work and why cloud computing is safer than local storage, it is imperative that we understand the possibilities and limits of AI and its products. No one is better equipped to explain that than those responsible for its development, and their role will be essential in helping everyone else understand what is at stake.

For all of this to happen, it is essential to approach regulation with the right mindset. There are two invaluable principles that form part of this mindset: one is that regulation must pass the progress-enabling test, and the other is that with great power comes great responsibility. Policymakers and regulators who devise or interpret regulation as a tool to restrain progress are victims of a failed zero-sum attitude. Looking at this issue as a safety vs. innovation or rights vs. technology choice is divisive and, therefore, unhelpful. Approaching digital regulatory policy as an enabler of progress will lead to much better and more desirable outcomes.

Equally, it is only right to acknowledge that developing or operating technology that has the potential to impact individuals and society brings with it huge responsibilities that cannot be ignored. Closing our eyes to this reality is only likely to provoke regulatory dogmatism, so it is in everyone's interest to be open and truthful about how technology is developed and what it is capable of doing. Ultimately, bridging any divide involves dialogue, and when dealing with new global technologies, that dialogue needs multiple perspectives and the ability to listen to each other.

Reporting ICT-related incidents and cyber threats under DORA: challenges and obstacles

Wim Nauwelaerts
Partner
wim.nauwelaerts@alston.com
Alston & Bird LLP, Brussels

Background

On January 17, 2025, the EU's Digital Operational Resilience Act (DORA) took effect. DORA establishes a comprehensive framework that regulates digital operational resilience for financial entities in the EU. It focuses on five key areas:

- management of ICT risks;
- management, classification, and reporting of ICT-related incidents;
- digital operational resilience testing;
- management of third-party risks and regulation of critical ICT service providers; and
- sharing of information on cyber threats.

DORA is a legislative initiative that follows the launch of the European Commission's 2018 FinTech Action Plan. According to the European Commission, finance has become predominantly digital, with profound interconnections and dependencies within the financial industry, as well as with third-party infrastructure and service providers.

In light of these developments, the European Commission has emphasized the need to enhance the resilience of the EU's financial sector, with a view to ensuring its technological safety and effectiveness, as well as its rapid recovery from ICT incidents. The overarching goal was to establish a regulatory framework that facilitates the seamless provision of financial services throughout the EU, even in times of stress, while maintaining consumer trust and confidence.

To this end, the European Commission identified a sector-specific initiative at the EU level as the most effective approach, one that would directly apply to financial entities within the EU. The Commission therefore adopted a proposal for a regulation (i.e., DORA), which consolidates and upgrades ICT risk requirements previously addressed separately in various EU and EU Member State legal acts. The aim of DORA was to address digital risk in the EU financial sector in a consistent manner and in a single legislative act.

Incident reporting is one of the areas for which the EU legislature wanted to introduce harmonized rules. Before DORA, ICT-related incident reporting thresholds and taxonomies varied significantly at the EU Member State level. As a result of these divergences, financial entities had to comply with multiple requirements across several EU Member States. The intention was therefore that DORA would provide a robust ICT-related incident reporting regime that addresses gaps in financial services laws, while at the same time removing existing overlaps and duplications.

DORA's reporting rules

DORA introduces requirements and rules on the reporting of major ICT-related incidents and significant cyber threats. A 'major ICT-related incident' (MICTI) is defined as an ICT-related incident that has a high adverse impact on the network and information systems that support critical or important functions of a financial entity. The notion

of 'significant cyber threat' (SCT) refers to cyber threats that could result in an MICTI or a major operational or security payment-related incident. To determine whether an incident or threat qualifies as an MICTI or SCT, financial entities will have to apply the classification criteria and materiality thresholds (specified in Commission Delegated Regulation (EU) 2024/1772) to their specific case. These criteria and thresholds take into consideration several factors, including clients, financial counterparties, and transactions affected by the incident, reputational impact, the duration of the incident, and any service downtime resulting from the incident.

Financial entities within scope of DORA are obligated to report MICTIs to the relevant competent authority using a staggered approach. They may, on a voluntary basis, notify SCTs to the competent authority when they consider the threat to be of relevance to the financial system, service users, or clients.

When an MICTI affects the financial interests of clients, financial entities must also inform their clients about the incident and the measures that the financial entity has implemented to mitigate the incident's adverse effects. In the event of an SCT, if financial entities decide to notify their clients voluntarily, they must also inform them of any appropriate protection measures that clients should consider taking.

Financial entities may outsource their reporting obligations under DORA to a third-party service provider, in which case the financial entities remain fully responsible for the fulfillment of DORA's incident reporting requirements.

DORA does not specify the content of reports, the time limit for notifications, or the procedures for reporting. However, it delegates authority to the European Commission to establish Regulatory Technical Standards (RTS) and Implementing Technical Standards (ITS) for harmonized reporting content, time limits, and templates.

To that effect, on February 20, 2025, the European Commission published the following regulations to supplement DORA's incident reporting rules:

- Commission Delegated Regulation (EU) 2025/301 for Regulatory Technical Standards on the content and time limits for the notification and reporting of MICTIs, and the content of voluntary notifications for SCTs (the Reporting RTS); and
- Commission Implementing Regulation (EU) 2025/302 for Implementing Technical Standards on standard forms, templates, and procedures for financial entities to report MICTIs and SCTs (the Reporting ITS).

Both the Reporting RTS and Reporting ITS became effective on March 12, 2025.

The Reporting RTS

The Reporting RTS contains additional rules on what information financial entities must report within what time limits in order to comply with DORA's reporting requirements. The Reporting RTS aims to provide a consistent approach for all types of financial entities, with a view to ensuring the harmonization and simplification of the notification and reporting requirements relating to MICTIs. The time limits for reporting MICTIs have also been largely aligned with the requirements set out in the NIS 2 Directive (Directive (EU) 2022/2555). The Reporting RTS imposes requirements on the content that needs to be included in the notifications and reports that are submitted to the relevant authorities. The submitted information should enable the authorities to further assess ICT-related incidents that have been reported and evaluate any supervisory actions they may want to take. As SCTs are notified on a voluntary basis, the content requirements for SCT notifications are less onerous than those that apply to the notification and reporting of MICTIs.

Mandatory reporting of MICTIs

- Financial entities are required to submit an initial notification to the relevant authority as early as possible, but no later than four hours from the classification of an ICT-related incident as an MICTI, and no later than 24 hours from the moment the financial entity has become aware of the ICT-related incident. This is an aggressive time frame, during which financial entities will have to compile, verify, and submit an extensive list of general and specific information, as required by the Reporting RTS. However, the Reporting RTS includes a more flexible regime that applies when a financial entity has not been able to classify an ICT-related incident as 'major' within 24 hours of becoming aware of the incident. In such cases, the financial entity may classify the ICT-related incident as major at a later stage, provided that it submits an initial notification to the relevant authority within four hours from the MICTI classification. This alternative approach is likely to become the default option for many financial entities that cannot realistically notify an MICTI within the first 24 hours.

- Following the initial notification, DORA requires that an intermediate report be submitted as soon as the status of the original incident has changed significantly or the handling of the MICTI has changed based on new information available. An intermediate report may also be due following a specific request of the relevant authority. Additionally, the Reporting RTS provides that financial entities must submit an intermediate report to the relevant authority within 72 hours of submitting the initial notification, even

if the status or handling of the incident remains unchanged. The Reporting RTS requires financial entities to submit an updated intermediate report if 'the regular activities have been recovered,' leaving uncertainty as to when this condition will be fulfilled in practice.

- A final report is due no later than one month after the submission of the latest updated intermediate report. In the final report, financial entities must include information about the root causes and resolution of the ICT-related incident, as well as any direct or indirect costs and losses resulting from the incident. It is important to note that in some cases, providing this level of detailed information within one month may not be feasible. It remains to be seen whether the competent authorities will apply leniency in these situations.

The Reporting RTS further stipulates that if a financial entity is unable to submit an initial notification, an intermediary report, or a final report within the prescribed time limits, it must inform the relevant authority without undue delay, but in no case later than the respective time limits for the submission of the notification or report. In such cases, the entity must also provide an explanation for the delay. It remains unclear which alternative time limits the authorities are expected to apply in these types of cases, and whether it will be possible to negotiate an 'extension' with the authorities. It is also uncertain whether, as a matter of best practice, financial entities that are unable to submit all of the required information (as listed in the Reporting RTS) within the prescribed time limits should request an extension - instead of submitting incomplete information.

The Reporting RTS includes another beneficial feature: if the time limits for submitting an initial notification, intermediate report, or final report fall on a weekend or bank holiday in the EU Member State of the reporting financial entity, the financial entity may notify or report by noon of the next working day. However, this extension is not available to credit institutions, central counterparties, operators of trading venues, and other financial entities that DORA has identified as essential or important entities.

The Reporting RTS does not include additional rules on when and how to inform clients about MICTIs. According to DORA, clients must be notified without undue delay, presumably after or at the same time as the initial notification to the competent authority. Further guidance from the authorities as regards the preferred timing for informing affected clients would be welcomed.

Voluntary notification of SCTs

The Reporting RTS does not address the timing of voluntary SCT notifications. DORA states that financial entities should notify SCTs 'when they deem the threat to be of relevance to the financial system, service users, or clients.' This implies that supervisory authorities will expect to receive SCT notifications shortly after the financial entity becomes aware of the threat. The Reporting RTS includes a lengthy list of topics that must be covered in the notification. This is somewhat strange, as SCT notifications are voluntary, and it may incentivize some financial entities to refrain from submitting SCT notifications. The Reporting RTS requires, for example, information about the potential impact of significant cyber threats on the financial entity, its clients, or financial counterparts. Financial entities would first have to perform an impact assessment, which may not be possible immediately after they become aware of the threat. Also, financial entities are expected to provide information about the status of the significant cyber threat and any changes in the threat activity. This assumes a threat evaluation over a certain period of time and raises questions as to how and when the authorities would need to be updated of any changes.

The Reporting ITS

The Reporting ITS includes a set of reporting templates, the use of which is mandatory. The templates are designed to ensure that financial entities can report MICTIs and SCTs to the authorities in a consistent manner and that they provide those authorities with data of good quality.

The Reporting ITS includes a 30-page template (with data glossary and instructions) for the purpose of reporting MICTIs. This template covers the initial notification, intermediate report, and final report required under DORA. Financial entities are required to make sure that the information entered into this template is complete and accurate. If accurate data is not available at the time of the initial notification or the immediate report, estimated values based on available information should be provided.

The Reporting ITS also specifies that financial entities must use secure electronic channels (as made available by the competent authority) to report MICTIs. In the event that secure electronic channels are unavailable, financial entities must notify the relevant authority of the MICTI through alternative secure means that have been approved by the authority.

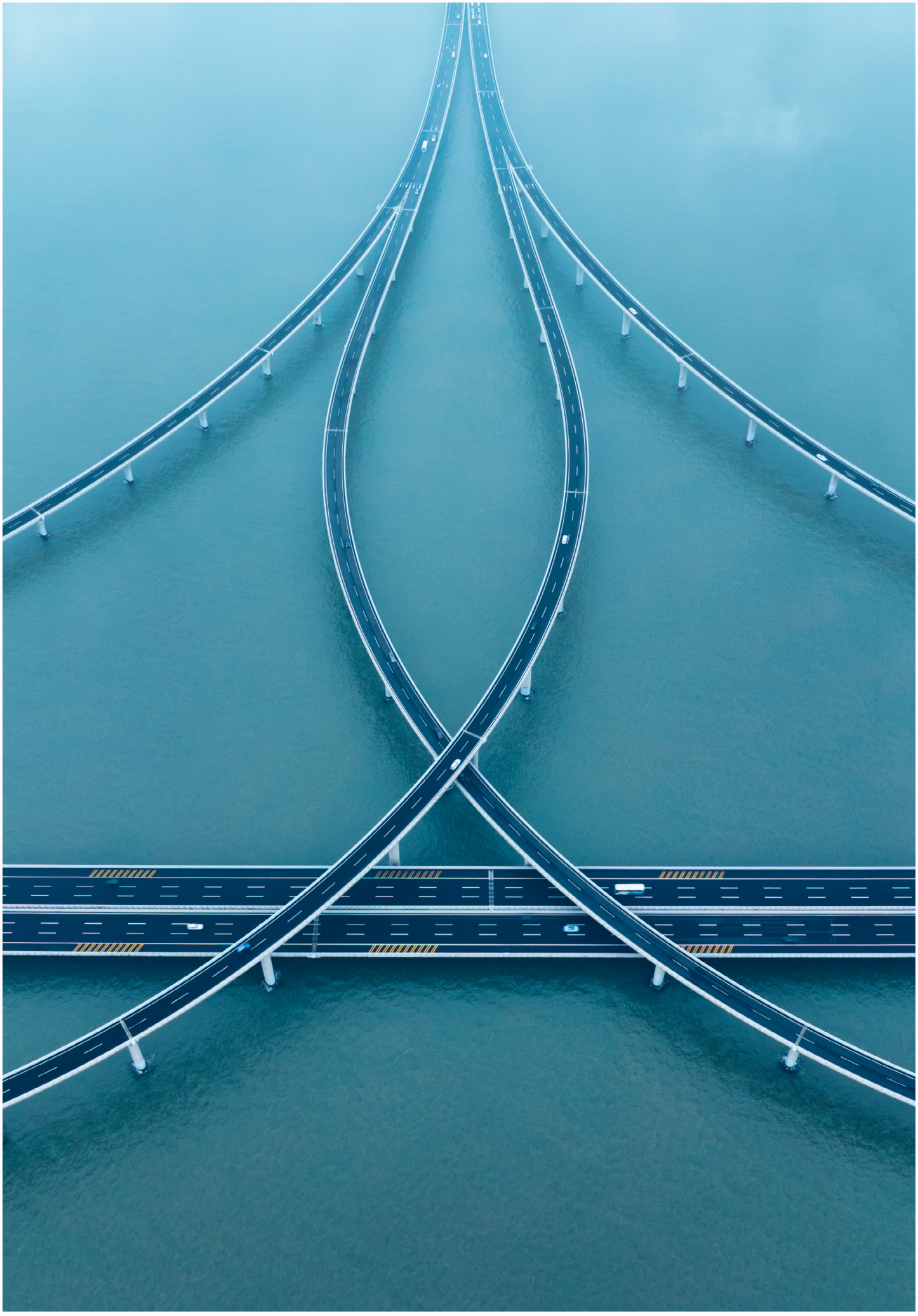
Under certain conditions, the submission of the initial notification, intermediate report, and final report may be consolidated into a joint submission to the competent authority. If a financial entity has reported an MICTI but, after further assessment, concludes that the incident does not fulfill the classification criteria and thresholds (set out in Commission Delegated Regulation (EU) 2024/1772), the financial entity should notify the authority about the reclassification using the template.

DORA provides financial entities with the option to outsource their MICTI reporting obligations to a third-party service provider. The Reporting ITS requires financial entities that have outsourced reporting obligations to inform the relevant authority of their outsourcing arrangement upon conclusion and no later than prior to the initial notification or reporting. Under specific conditions, a third-party service provider may submit a single notification or report on behalf of multiple entities affected by the same MICTI. This type of aggregated reporting may be relevant in cases where an MICTI impacts several financial entities and originates from or is caused by the same third-party ICT service provider. However, if the authorities require specific information about an impacted financial entity, they may still require that entity to submit an individual notification or report.

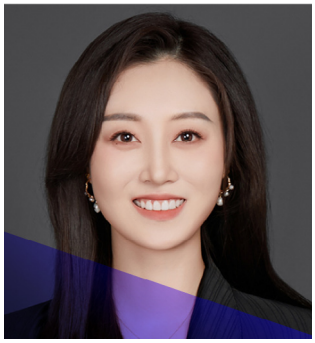
Financial entities that voluntarily notify SCTs must use the specific template, data glossary, and instructions included in the Reporting ITS, and they will have to ensure that the information included in the template and subsequently submitted to the authority is complete and accurate.

Concluding remarks

Financial entities are likely to embrace DORA's new harmonized rules on incident and threat reporting. However, despite the additional reporting standards and templates that the European Commission has recently made available, it will not always be clear when and how to submit reports and notifications in compliance with DORA. It would be useful if the relevant authorities could issue further guidance, in particular on the time limits and possible extensions that apply to the different reporting stages. In addition, if an ICT-related incident involves personal data - which will often be the case - the incident could also constitute a personal data breach for purposes of the General Data Protection Regulation (GDPR). In that case, financial entities may be required to submit separate notifications to different regulators under both DORA and the GDPR, with diverging time limits and procedural obligations. DORA could (and perhaps should) have included a one-stop shop for ICT-related incidents that qualify as personal data breaches. This is clearly a missed opportunity.



APAC: Key developments of 2024 - part two



Fengming Jin
Associate
Fengming.Jin@twobirds.com
Bird & Bird, Beijing

James Gong
Partner
James.Gong@twobirds.com
Bird & Bird, Beijing

Wilfred Ng
Partner
Wilfred.Ng@twobirds.com
Bird & Bird, Hong Kong

Hwee Yong Neo
Senior Managing Associate
HweeYong.Neo@twobirds.com
Bird & Bird, Hong Kong

China's Mainland

Overview

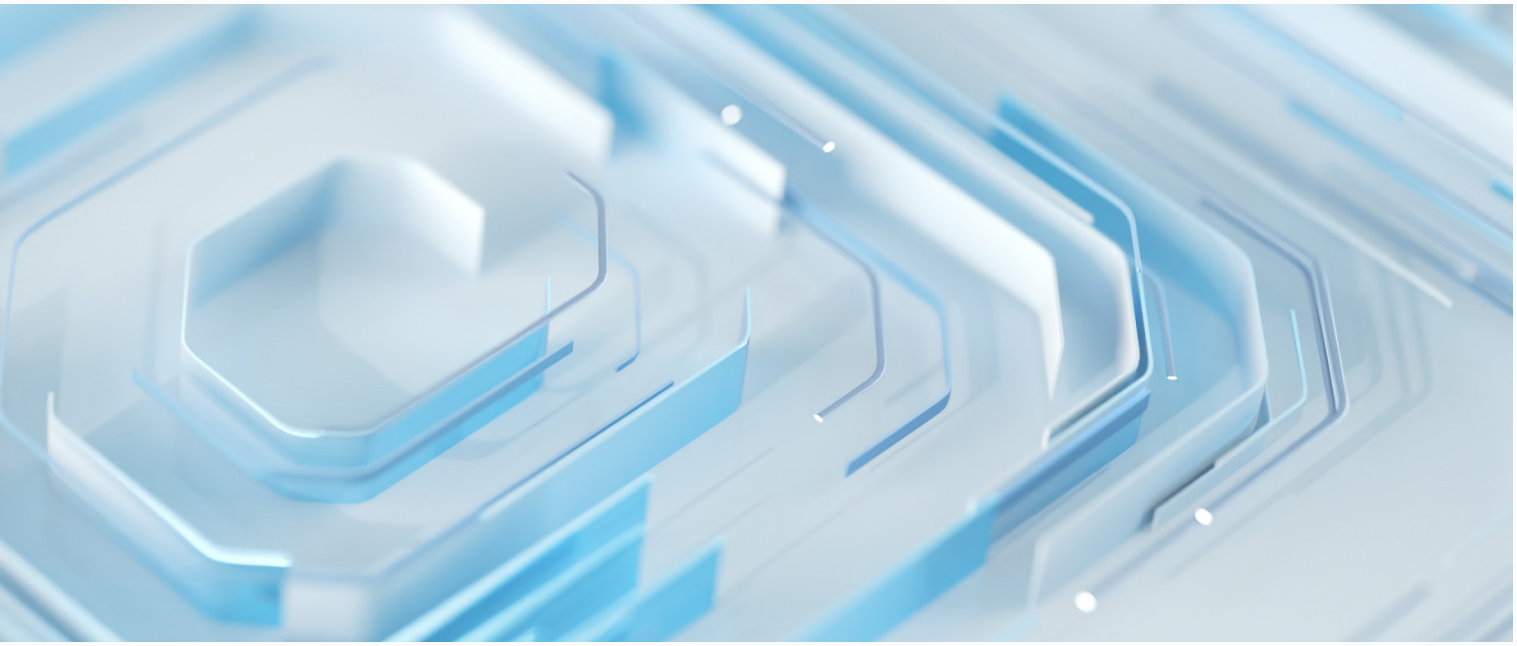
In 2024, China's data protection and cybersecurity legislation matured significantly. New regulations were introduced to support the implementation of the three-pillar data protection laws, covering various aspects including personal information protection audits, cyber and data security, as well as the identification of sensitive personal information. One noteworthy aspect in 2024 in China concerning data protection is the regulatory developments related to data export.

Regarding artificial intelligence (AI), China has yet to establish a unified AI-specific law. Currently, the essential regulations in the AI sector include several regulations issued in 2022 and 2023. In 2024, the development of AI-related normative documents flourished, with national and local governments implementing measures to enhance AI management and application, promoting high-quality and standardized development.

In the following section on China, we first elaborate on the major advancements in AI in 2024. Then we will discuss the significant developments in data protection, focusing on general data protection and cross-border data transfer regulations.

AI framework

China has yet to establish a unified law specifically for AI. Currently, the



three primary regulations governing the AI sector include the Regulations on the Management of Algorithmic Recommendations for Internet Information Services (the Algorithm Regulations), released in 2022, the Interim Measures for the Administration of Generative Artificial Intelligence Services (the Generative AI Measures), and the Regulations on the Administration of Deep Synthesis for Internet Information Services (the Deep Synthesis Regulations) released in 2023. These three regulations mark China's initial steps in AI governance and lay the groundwork for future AI regulation. To recap, we briefly summarize the AI framework constituted by the three regulations as follows.

- **The Algorithm Regulations** apply to activities in China using recommendation algorithm technology for internet information services, including AI services. Key obligations include the following.
  - Algorithm safety: Providers of algorithm recommendation services must implement management and technical measures, such as algorithm audits, ethical reviews, data security, and emergency response plans.
  - Filing requirement: Algorithm recommendation services with public influence must file their information within 10 business days of launch.
  - Information security management: Providers must manage platforms actively, prioritize mainstream values, ensure algorithm transparency, detect and label synthetic content, halt illegal content, report violations, and manage disputes.
- **The Generative AI Measures** were issued by the Cyberspace Administration of China (CAC) and six other departments, and apply to services using generative AI to provide content like text, images, audio, and video. Key provisions include the following.
  - Content governance: Providers must ensure AI-generated content complies with Chinese laws and values, is non-discriminatory, accurate, and true. Non-compliant content must be addressed, reported, and labelled as AI-generated.
  - AI training compliance: Training data must be lawful, protect IP rights, comply with cybersecurity and data protection laws, and ensure diversity. Personal data use requires legal permission or consent. Clear labelling and anti-discrimination measures are mandatory.
  - Government oversight: Services with social influence must undergo security assessments and algorithm registration with the CAC. Ethical reviews focus on safety, fairness, transparency, reliability, and controllability.
- **The Deep Synthesis Regulations** apply to activities in China using deep synthesis technology for internet information services, including AI. The deep synthesis technology refers to technology that generates content through algorithms based on deep learning and virtual reality. Key points include the following.
  - Identity verification: Service providers must verify users' real identities using mobile numbers, ID numbers, or social credit codes. Without verification, service providers are prohibited from offering information publishing services.
  - Content management: Providers must manage harmful content, review data and outputs, report issues, and apply warnings or suspensions if needed. They must also maintain rumor correction and complaint channels and report false information to authorities.
  - Algorithm filing and security assessment: Providers and technology supporters with public influence must file algorithms and publish this filing. New products or functions with similar capabilities require a security assessment.

In 2024, a plethora of AI normative regulations emerged. Governmental and industrial authorities introduced national AI standards and regulations to guide industry development. With measures implemented by national and local governments, we observe actions covering various aspects conducted, including releasing cybersecurity standards plans, seeking opinions on AI industry standards, and adjudicating the first AI-generated artwork copyright infringement case, etc. These actions aim to elevate AI technology standardization, foster industry innovation, enhance regulatory efficiency, and drive intelligent development across various sectors. We summarize these documents as follows.

- The Basic Security Requirements for Generative Artificial Intelligence Services provide detailed guidance on the security requirements for generative AI services and evaluation tools for AI safety regulation, including large model filings. This serves as a reference for generative AI service providers to conduct security assessments and enhance safety levels. It addresses gaps in the Generative AI Measures regarding specific security requirements, evaluation parameters, and standards for large model filings.
- The AI Security Governance Framework 1.0 addresses AI security and data protection with principles like 'Inclusive Prudence' and 'Risk-Driven Governance.' It also recommends measures to manage AI risks, including algorithmic bias, data breaches, system vulnerabilities, and ethical issues.
- The Security Specification for Generative AI Pre-Training and Fine-Tuning Data (Draft) also outlines security requirements for data handling in generative AI, covering data classification, source documentation,

security monitoring, access control, encryption, and backup, and includes audit and emergency response protocols to ensure compliance.
- The Generative AI Data Annotation Security Specification (Draft) sets security requirements for data handling in AI-generated content and lays down responsibilities with a focus on AI data annotation, including data classification, source documentation, security monitoring, identity verification, access control, encryption, and backup, covering audit trails, compliance tracking, and emergency response protocols.
- The Labelling Method for AI-Generated Content (Draft) provides guidelines for labelling AI-generated synthetic content via defining explicit labels (text, sound, and graphics) and implicit labels (embedded metadata). This document focuses on ensuring transparency and traceability of AI-generated content for service providers and content distribution platforms.

These standards complement and extend the previous three AI regulations, fostering their further implementation. Notably, all initiatives emphasize safety, compliance, and standardization, providing robust support for the healthy development of China's AI industry.

Data and cybersecurity law

China's data protection legal framework is anchored by so-called 'three pillar laws,' namely, the Personal Information Protection Law (PIPL), the Data Security Law (DSL), and the Cybersecurity Law (CSL). Complementing these are various administrative regulations, departmental guidelines, and national standards. Specific sectors, such as healthcare, telecommunications, finance, and automotive, etc., also have tailored legislation impacting data protection. Significant developments in 2024 are elaborated as follows.

1. General data protection

The State Council released the Regulations on the Management of Network Data Security (Management Regulation) on September 30, 2024, effective from January 1, 2025. Network data refers to various types of electronic data processed and generated through networks. This Management Regulation is grounded in higher-level laws such as the PIPL, CSL, and DSL. It elaborates on the procedural and substantive aspects of the principles and systems established by the three pillar laws, aiming to standardize network data processing activities, ensure data security, promote lawful and reasonable use of data, protect individual and organizational rights, and safeguard national security and public interests. Specifically, this document comprises nine chapters and 64 articles, and the main provisions are as follows.

- General requirements for network data security management: It encourages innovative use of network data, requests implementation of classified protection, encourages participation in international rulemaking, strengthens industry self-regulation, and prohibits illegal data processing. It also requires data controllers to establish security management systems, report risks, and handle incidents.
- Personal information protection: It clarifies rules for processing personal information, mandates convenient methods for individuals to exercise their rights, and prohibits unreasonable restrictions. It also specifies obligations for automated data collection and handling personal information transfer requests.
- Perfection on security of important data: It defines responsibilities for creating important data catalogues, requires identification and reporting of important data, outlines responsibilities of security management agencies and officers, and specifies risk assessment requirements.
- Optimization of network data export security management: It clarifies conditions for providing personal information overseas, allows data transfer under international treaties, and states that data not identified or publicly announced as important data by relevant regions or departments does not need to be declared as important data for the governmental assessment.
- Obligations of network platform service providers: It specifies security requirements for platform and third-party providers, clarifies rules for automated decision-making, and requires large network platform service providers to publish annual reports on their social responsibility for personal information protection and to prevent cross-border network data security risks.

While the long-anticipated Management Regulations have finally been implemented, we observe a clear trend in 2024 regulations from a general data protection perspective that those regulations extend and build upon the provisions and guidelines established or that have been proposed in 2023. For example, the Data Security Technology - Personal Information Protection Compliance Audit Requirements (Draft for Comment) issued on July 12, 2024, not only elaborates on the compliance audit obligations of personal information controllers as outlined in Article 54 of the PIPL but also reinforces the Personal Information Protection Compliance Audit Management Measures (Draft for Comment) from 2023. This draft introduces a comprehensive suite of compliance audit tools and templates, including a personal information compliance audit process and a personal information protection compliance audit report template.

This trend underscores the continuity in China's general data protection legislation and highlights the increasing sophistication and maturity of its data protection laws.

2. Regulations on data export

One noteworthy aspect in 2024 in China concerning data protection is the regulatory development related to data export. We have discussed the data export regime in China comprehensively in our July Data Protection Leader article. For a quick recap, before 2024, under the PIPL, a personal information controller may only export personal information after satisfying one of the following data export safeguard routes:
- passing a CAC approved security assessment concerning data export activities (Governmental Assessment);
- obtaining a personal information protection certification provided by competent authorities (Protection Certification); or
- executing standard contract clauses with personal information importers and filing such contract along with other materials with the local CACs (SCCs Filing).

The three routes have raised concerns among multinational companies due to their complex, unpredictable nature and the uncertainty about their impact on data export during normal business operations. In response, the CAC released the Regulation on Promoting and Regulating Cross-border Data Flow (the Regulation), along with updated guidelines on Governmental Assessment and SCCs Filing, aiming to relax the rules for exporting personal information from China. Based on our current project experience, even without being exempted by the Regulation, many companies that previously needed to undergo the more complex Governmental Assessment process now only need to follow the SCCs Filing procedure. Additionally, when using the simplified template to conduct the Personal Information Protection Impact Assessment for SCCs Filing, the local CACs have relaxed the requirements for supporting documentation compared to before, significantly improving review and feedback times.

Moreover, to further facilitate data export, since June 29, 2023, the CAC and the Innovation, Technology and Industry Bureau (ITIB) of the Hong Kong Government have signed the 'Memorandum of Understanding on Facilitating Cross-boundary Data Flow within the Guangdong-Hong Kong-Macao Greater Bay Area.' This agreement aims to establish a secure mechanism for cross-border data flow in the Greater Bay Area, within the national framework for safeguarding the security of cross-border data transfers.

In line with this intention, on December 13, 2023, the Implementation Guidelines for Standard Contract for the Cross-boundary Flow of Personal Information Within the Guangdong-Hong Kong-Macao

Greater Bay Area (Mainland, Hong Kong) (GBA SCC Guidelines) were jointly issued by the CAC and ITIB of the Hong Kong Government. These guidelines offer an alternative route for cross-border data transfers within the GBA by allowing the voluntary adoption of the GBA SCCs. Moreover, according to the Regulation, pilot free trade zones can independently formulate 'negative lists' of data that require Governmental Assessment, Protection Certification, and SCCs Filing, within the framework of the national data classification and grading protection system, exempting non-listed data from outbound filing processes. These 'negative lists' are implemented after approval through the proper procedures. In 2024, the respective pilot free trade zones in Shanghai, Tianjin, and Beijing have issued relevant measures for data export within the free trade zones, providing negative lists as well as guidelines for cross-border data transfers within these zones.

Hong Kong

Overview

Hong Kong is aligning with the global trend of enhanced guidance for AI development, alongside strengthened cybersecurity legislation. In conjunction with proposed amendments of the privacy law, the introduction of the Model Framework (defined below) and the proposed new cybersecurity law aim to position Hong Kong as a global infotech hub that fosters innovation while ensuring robust protections for personal data and critical infrastructure.

AI framework

On June 11, 2024, the Office of the Privacy Commissioner for Personal Data (PCPD) in Hong Kong released the 'Artificial Intelligence: Model Personal Data Protection Framework' (Model Framework). This document is aimed at organizations that procure, implement, and use AI systems from third parties, ensuring their compliance with the Personal Data (Privacy) Ordinance (PDPO). The Model Framework does not apply to firms that develop AI in-house. This is instead covered in the 'Guidance on the Ethical Development and Use of Artificial Intelligence' previously issued by PCPD in August 2021.

The Model Framework covers both predictive and generative AI, addressing best practices for managing personal data during the lifecycle of AI systems. The key aspects of the Model Framework as well as the main implications and observations for data users are set out below.

1. Recommended compliance:
   - Organizations should adhere to key privacy and security obligations (as controller, joint controller, or processor in underlying data processing activity) throughout the entire lifecycle of AI systems. For example, if AI system providers are engaged as processors, the requisite contractual obligations to be imposed on security and unnecessary retention would apply.
   - Organizations should create an AI Incident Response Plan to manage risks effectively, which should include a notification mechanism to inform internal stakeholders and external affected parties, such as data subjects and regulatory authorities, depending on the severity of the incident and applicable regulatory requirements.

2. Risk-based approach:
   - The Model Framework advocates for a risk-based strategy to use and procure AI systems so that the relevant risks, including privacy risks, involved in the process can be systematically identified, analyzed, and evaluated.
   - Notable examples under this approach include recommendations where organizations should consider:
     - forming an AI governance committee to oversee the procurement and implementation process of AI solutions; and
     - conducting a Privacy Impact Assessment (PIA) before deploying AI systems, particularly when sensitive data is involved.
   - When using personal data for training or customization, data users must consider whether such use is allowed, whether the volume of data used is necessary, and the sensitivity of the data involved.

3. Regulatory attention:
   - Organizations should monitor both operational changes and regulatory development in the context of AI, as the PCPD has conducted compliance checks on 28 organizations regarding the implications of the development or use of AI across various sectors.

4. Explainable AI:
   - Transparency and accountability obligations require a thorough understanding of AI systems. Data users should therefore adopt a proactive approach to clearly explain the relevant information (e.g., privacy risks and impact of automated processing) to data subjects in a comprehensible manner.

Cybersecurity law

On June 25, 2024, new cybersecurity legislation to enhance the protection of computer systems of critical infrastructures (CI) was proposed by the Hong Kong Government. The legislation is tentatively titled the Protection of Critical Infrastructure (Computer System) Bill (the Bill). The one-month consultation period for the Bill ended on August 1, and a consultation report was published by the Hong Kong Government on October 8 (Consultation Report). The Bill targets CI operators (CIOs) in Hong Kong that are necessary for
- the continuous delivery of essential services; and
- maintaining important societal and economic activities.

The Bill requires organizations upon designation by the newly established Commissioner's Office (the Office) under the Security Bureau to take appropriate measures to strengthen the security of their computer systems. The Office is empowered to investigate and enforce non-compliance with the proposed obligations, and to designate industry-specific regulators of essential service sectors such as the Monetary Authority and Communications Authority to monitor compliance.

It should be noted that only the Critical Computer Systems (CCSs) of CIOs will be regulated. CCSs are systems which are necessary for the provision of essential services and those systems which, if interrupted, will seriously impact the normal functioning of the CIs. Once designated, the statutory obligations will apply to the CCSs regardless of whether they are physically located in Hong Kong or elsewhere. In the Consultation Report, the Security Bureau stated that the Office will determine whether a CIO or CCS designation is suitable through mutual communication and understanding with the operators.

The Bill will adopt an 'organization-based' approach in two respects:
- the list of the designated CIOs will not be disclosed under the proposed legislation but rather only the names of the eight essential service sectors will be set out; and
- non-compliance will be an offense for the organizations but not on the heads or staff of the CIOs at the individual level.

The key obligations of CIOs are outlined below.

1. Organizational obligations
- Keep the Office updated on the ownership and operatorship of CI.
- Appoint a dedicated team with professional knowledge to manage cybersecurity.

In the Consultation Report, the Government stated that:
- it would seriously consider removing the requirement to update the Office on ownership given the concerns on practical difficulties expressed by a number of respondents; and
- in light of concerns over difficulties in hiring competent personnel, it would not stipulate the statutory qualification requirements of computer system security personnel and would instead compile a list of eligible professional qualifications in the code of practice.

2. Preventive obligations
- Inform the Office of any material changes to CCSs.
- Develop and submit a comprehensive computer system security management plan to the Office.
- Conduct annual risk assessments,

perform independent audits every two years, and report both findings back to the Office.
- Ensure their CCSs' compliance while engaging third-party service providers.

In the Consultation Report, the Government stated that:
- the reporting of material changes is not targeted as personal data or commercial confidential information, but rather to ensure operators are compliant and for the Office to conduct proper assessment of incidents; and
- audits and assessment criteria will be based on the latest technology and international standards, and audits must be conducted by independent third parties.

3. Incident reporting and response obligations
- Take part in a security drill for computer systems organized by the Office at least once every two years.
- Develop and submit an emergency response plan for security incidents within three months of designation to the Office.
- Report security incidents to the Office within specified time frames (e.g., serious incidents within two hours).

In the Consultation Report, the Government stated that, in relation to the reporting of serious incident within two hours, in light of respondents' concerns the Government would seriously consider extending the time frame to 12 hours, and as for other incidents the time frame could be relaxed from 24 hours to 48 hours after being aware of the same.

The obligations will apply to all CCSs, regardless of whether they are physically located in Hong Kong or not. In addition, upon request by the Office in the course of investigating an incident or offense, CIOs must submit relevant information available to them, even if such information is located outside Hong Kong.

The Bill, gazetted on December 6, 2024, was introduced to the Legislative Council and read for the first time on December 11, 2024. The Government aims to establish the Office within a year of the Bill's passage, with the legislation taking effect six months later. In the meantime, the Government will continue to liaise with stakeholders from various sectors and jointly develop a code of practice that is applicable to the sectors.

Directions for the next PDPO Amendment

The previous amendments to the PDPO were aimed at strengthening the combat against unlawful doxing acts (i.e., gathering personal data of target individual(s) through online resources and disclosing such data on the internet). The Personal Data (Privacy) (Amendment) Ordinance 2021 came into effect on October 8, 2021, which empowers the Privacy Commissioner to carry out criminal investigations, institute prosecutions, and issue cessation notices in relation to doxing-related offenses. As at the date of this article, a concrete proposal on further amendments to the PDPO is yet to be formulated by the PCPD. However, in its responses to the Legislative Council's query on the timeline for the next legislative amendment exercise, the PCPD shared that its current directions of the amendment exercise included the following:
- establishing a mandatory data breach notification mechanism;
- requiring data users to formulate a data retention period policy;
- empowering the PCPD to impose administrative fines; and
- regulating data processors directly.

Macau

The primary legislation governing data protection in Macau is the Personal Data Protection Law, enacted in 2005. Additionally, the Public Places Video Surveillance Legal System (Law No. 2/2012) serves as a specialized law in this field. The regulatory authority, the Office for Personal Data Protection, has also issued a series of guidelines focusing on data protection.

Although Macau's data protection legislation began early, its development has been relatively slow. Notably, on September 10, 2024, the CAC, the Economic and Technological Development Bureau of the Macau SAR Government, and the Office for Personal Data Protection of the Macau SAR Government jointly issued the Guidelines for the Implementation of Standard Contracts for Cross-Border Transfer of Personal Information in the Guangdong-Hong Kong-Macao Greater Bay Area (Mainland and Macau). Accompanying these guidelines were templates for the Standard Contract and the Commitment Letter. These documents will facilitate the personal information transfer between China's Mainland and Macau. In the realm of AI, Macau currently lacks AI-specific laws.

Thailand

Overview

Thailand has established data protection and cybersecurity laws to safeguard personal data and ensure cybersecurity. The Personal Data Protection Act (PDPA), effective since June 2022, regulates the collection, usage, and transfer of personal data, granting individuals rights such as access and correction. The Cybersecurity Act, enacted in 2019, focuses on protecting critical information infrastructure and mandates compliance with cybersecurity standards. Recent developments include new regulations on cross-border data transfers, enhancing the legal framework. Thailand currently does not have any enacted AI laws, but two significant draft bills are under review.

AI framework
- Draft Royal Decree on Business Operations Using Artificial Intelligence Systems: Proposed by the Office of the National Digital Economy and Society Commission, the Draft Royal Decree is to be issued under the Electronic Transactions Act, B.E. 2544 (2001) (ETA). The Draft Royal Decree aims to implement control and prevention measures based on the severity of potential effects from AI-operated service businesses, build trust in electronic data systems, and prevent public harm. Influenced by the then-draft EU AI Act, the Draft Royal Decree underwent a public hearing in October 2022.
- Draft Act on Thailand Artificial Intelligence Promotion and Support: In addition to the Draft Royal Decree, the Electronic Transactions Development Agency (ETDA) sought public feedback in July 2023 on the Draft Act on Promotion and Support for Artificial Intelligence in Thailand, along with two draft sub-regulations, namely the ETDA Notification on Risk Assessment from the Use of AI Systems and the ETDA Notification on AI Sandbox. These drafts aim to enhance AI development by providing a regulatory sandbox, relaxing or exempting certain laws, and offering support from relevant authorities.

In the meantime, on March 22, 2022, the National Science and Technology Development Agency approved ethical guidelines for AI. These guidelines are released to ensure that AI technologies and data science, including AI-driven algorithms, are developed and used ethically.

Data protection and cybersecurity law

On December 25, 2023, Thailand's Personal Data Protection Committee (PDPC) published two subordinate regulations regarding the cross-border transfer of personal data under the PDPA. Both regulations came into force on March 24, 2024. The highlights of these two regulations are highlighted as follows.
- Whitelist Notification: The newly issued Whitelist Notification outlines the criteria for the PDPC to determine whether a destination country or international organization has 'adequate' personal data protection standards, such as the existence of legal measures in the destination country. However, the PDPC has not yet announced the list of Whitelisted Countries.
- Binding Corporate Rules (BCRs): The regulations detailed the procedures for submitting BCRs to the Office of the PDPC for review and approval. This includes the binding effect and mandatory minimum provisions required.
- Appropriate safeguards: The regulations further specify the appropriate safeguards to be used if the PDPC does not recognize a particular country as having adequate data protection standards or if BCRs

are not relied upon. These safeguards include Standard Contractual Clauses (SCCs), certification, and binding instruments between foreign government agencies and local entities.

In 2024, the PDPC also issued a series of documents, including announcements and decrees, providing guidance on the implementation of the PDPA. These documents cover topics such as the procedures for exercising the right to deletion and exemptions from certain obligations for data controllers. Additionally, on April 29, 2024, the PDPC released its four-year plan emphasizing the development and enhancement of the data protection framework in Thailand from 2024 to 2027.

Vietnam

Overview

Prior to July 1, 2023, rules and regulations on personal data protection were dispersed across various laws, including general laws such as the Civil Code 2015 and the Law on Cyber Information Security No. 86/2015/QH13, as well as sector-specific laws. On April 17, 2023, the Government of Vietnam issued Decree No. 13/2023/ND-CP on the Protection of Personal Data (PDPD), which came into effect on July 1, 2023. In 2024, the Vietnamese Government introduced a series of draft laws and regulations related to data protection, aiming to further enhance data protection capabilities while ensuring data rights and data flow.

Vietnam does not have specific laws governing AI. Currently, the AI-related legislation is the draft Law on Digital Technology Industry, announced by the Ministry of Information and Communications in July 2024.

AI framework

On July 2, 2024, Vietnam's Ministry of Information and Communications released the Vietnam Digital Technology Industry Law (VDTI Law) draft for public consultation. This law aims to support and regulate the digital technology sector, with a particular emphasis on AI as a key area of enforcement, recognizing its vital role in driving economic growth and establishing the digital technology industry as a core pillar of the national economy.

The draft defines AI systems, categorizes risk levels, and sets out management measures and ethical principles for AI. Key highlights may include the following.

1. **Prioritizing AI enforcement**

- The draft VDTI Law seeks to support the development and application of AI, while also establishing ethical standards and restrictions for AI practices. Using a risk-based governance approach, the draft allocates compliance responsibilities based on the risk profiles of AI systems and provides a framework for the safe and responsible development and deployment of AI.
- As part of this framework, certain types of AI systems are prohibited, such as those that manipulate individual behaviors at a subconscious level, discriminate against specific groups based on social behavior (i.e., social credit scoring), engage in large-scale facial recognition surveillance, or infer human emotions in workplaces or educational settings.

2. **Regulatory sandbox for innovative digital technologies**

- The draft VDTI Law introduces a sandbox mechanism that allows for the temporary testing of pioneering digital technology products and services in a controlled environment.
- This mechanism facilitates the assessment of the costs and benefits of innovative technologies, thereby strengthening risk management prior to broader implementation.

This draft legislation demonstrates Vietnam's commitment to fostering innovation in the digital sector while safeguarding ethical and responsible technological advancement.

Data protection and cybersecurity laws

On November 30, 2024, the Ministry of Public Security (MPS) announced the passage of the Data Law, following its unveiling on July 1, 2024. The Data Law enters into effect on July 1, 2025. The Data Law aspires to foster unified, consistent, and effective data usage for national governance. In essence, the draft Data Law lays the groundwork for the establishment, operation, and utilization of the National Synthesis Database at the National Data Centre, as well as the requirements for specific forms of data processing, applicable to both state entities and private enterprises. It is noteworthy that the draft Data Law emphasizes the strict regulation of cross-border data transfers, especially those involving 'core data' and 'important data,' will be subject to stricter regulations. After a data security assessment, the data export of core data and important data would require approval from relevant authorities before being transferred across borders. This measure aims to mitigate risks to national security and public interests while allowing the free flow of data across borders under secure conditions.

Moreover, on September 24, 2024, the MPS opened the draft Personal Data Protection Law (PDPL) for public consultation. This draft comprises seven chapters and 68 articles and is scheduled to come into effect on January 1, 2026. The PDPL draft is more comprehensive, covering a broader range of areas such as big data processing, AI, cloud computing, financial and credit data, healthcare, and insurance.

- Key highlights of the PDPL include stricter consent requirements, which explicitly provided that the consent of the data subject must be given through an affirmative action that provides a clear and specific indication, such as in writing, verbally, by ticking a consent box, using a consent syntax via message, selecting consent settings, or through another action that demonstrates this; silence or non-response cannot be considered consent.
- Furthermore, the PDPL provides more detailed rules concerning data export. It first defines the cases that constitute data export, followed by the obligations imposed on organizations engaging in data export to adhere to multiple compliance measures. For instance, before initiating any transfer, organizations must conduct a data export impact assessment and develop a report accordingly. The PDPL further lists the information required to be included in this report and the timeline for submitting this report to the relevant authorities.
- The PDPL also attempts to regulate various other aspects such as big data processing, AI, and cloud computing. It emphasizes data subjects' right to opt out of AI-based automated decisions to mitigate any negative effects algorithms may cause. Data usage requires the explicit, informed consent of the data subject, with clear explanations provided to secure their right to choose and be informed.

Building a data protection and AI compliance program

©Sane Seven

Dr. Sachiko Scheuing
European Privacy Officer, Acxiom

Building a data protection and AI compliance program

New Chief Privacy Officers (CPOs) and data protection officers (DPOs) often take up the major challenge of developing and implementing a robust data protection compliance program. This article offers guidance on this complex undertaking, exploring relevant frameworks for data protection and artificial intelligence (AI) compliance, and providing practical organizational insights for successful implementation.

Why develop a compliance program?

A compliance program is a structured framework within an organization designed to ensure adherence to legal, regulatory, and ethical standards. It is a holistic system that integrates policies, procedures, and controls to promote a culture of integrity, accountability, and risk management. Data protection compliance programs often work alongside other compliance initiatives addressing industry-specific regulations, e.g., the Digital Operational Resilience Act (DORA), Health Insurance Portability and Accountability Act (HIPAA), etc., or departmental standards (e.g., HR, Finance, etc.).

Effective data protection programs mitigate legal and financial risks, protect reputation, and ensure regulatory compliance. They also foster a culture of ethical conduct, building stakeholder trust.

External experts - specialized law firms, data protection consultants, and privacy tech companies - offer valuable assistance, drawing on their extensive experience in building and implementing compliance programs. Their insights can also be helpful in navigating internal communications, especially with senior management. However, internal stakeholders, including the DPO or CPO, must provide crucial business knowledge and understanding of the organization's internal dynamics when working with external advisors.

Framework for a robust compliance program

Developing a compliance program becomes more manageable when using a trusted framework to guide the process. External advisors may also have a preferred framework to work with. Using established frameworks offers two main advantages: first, there is assurance that all major aspects of a compliance program are addressed; second, regulators and auditors are familiar with the approach, which makes it easier for them to assess the robustness of your organization's compliance program.

The CIPL Accountability Framework, also known as the Accountability Wheel, is one such framework. The Accountability Wheel serves as a model for developing comprehensive privacy and data governance programs, globally.

The framework has seven core elements:

1. **Leadership and oversight:** Commitment from the top, and subsequently from all levels of management. A suitable individual, CPO or a DPO, to be appointed to oversee the compliance program and report to the board.
2. **Risk assessment:** Assessing and mitigating risks to data subjects, weighing them against the benefits. Periodic risk reviews of the overall privacy program should be conducted to ensure the compliance program is adjusted to fluctuating risk levels, resulting from changes in law, business models, and technology.
3. **Policies and procedures:** Develop internal policies and procedures that operationalize legal requirements, industry standards, and the organization's values and goals.
4. **Transparency:** Provide stakeholders (internal and external) information about the organization's privacy program, procedures, data use, and data subject rights.
5. **Training and awareness:** Train employees and raise awareness of the internal privacy program, its objectives, requirements, and individual responsibilities. The importance of data protection to be rooted in a culture of shared responsibility.
6. **Monitoring and verification:** Ongoing monitoring to measure program effectiveness through regular audits and, where necessary, the development of redress plans.
7. **Response and enforcement:** Implementation of response and enforcement procedures to handle inquiries, breaches, and internal non-compliance.

The synergy of these seven elements creates a robust compliance basis embedded in an accountable culture. While widely adopted by global organizations, mostly with mature privacy governance programs, the framework's components are universal and scalable, making it useful for SMEs as well.

Building a data protection compliance program in the age of AI

The explosive growth of AI, significantly accelerated by the public release of ChatGPT in late 2022, has fundamentally reshaped the technological landscape. This rapid expansion of AI's capabilities and applications across various sectors has created a surge in demand for expertise in AI governance and compliance. Organizations are increasingly recognizing the critical need to integrate AI considerations into their broader data protection strategies, leading to a significant expansion of the roles and responsibilities of CPOs and DPOs.

Many organizations are finding that their existing data protection teams are uniquely positioned to address the complexities of AI governance. These teams are equipped with a deep understanding of data privacy regulations, risk assessment methodologies, and the ethical implications of data processing - all crucial elements in navigating the challenges presented by AI systems. Many CPOs and DPOs are now tasked not only with traditional data protection responsibilities, but also with spearheading the development and implementation of comprehensive AI accountability programs within their organizations. These added responsibilities of CPOs and DPOs recognize the synergistic relationship between data protection and AI governance, leveraging existing expertise to address the emerging challenges.

However, it is crucial to acknowledge that while significant overlaps exist between data protection and AI governance, there are also fundamental differences that require careful consideration. A direct comparison of the General Data Protection Regulation (GDPR) and the EU AI Act serves to illustrate these differences. The GDPR aims to protect the right to data protection, enshrined in Article 8 of the Charter of Fundamental Rights of the European Union. The EU AI Act, on the other hand, is primarily a product safety law for AI systems. It aims to ensure that AI systems are developed and deployed safely. Its built-in risk assessment approach, classifying AI as prohibited, high-risk, or minimal risk, resembles safety standards used in, for instance, manufacturing household appliances or producing food.

Arguably, the impact of AI systems can be broader than that of processing personal data. Therefore, assessments, when required by law, become more extensive. For instance, a Data Protection Impact Assessment (DPIA), required under the GDPR for high-risk processing, examines the risk to the rights and freedoms of the data subject, with an emphasis on the right to data protection. For high-risk AI systems involving personal data, a Fundamental Rights Impact Assessment (FRIA) may be required, on top of a DPIA. Another notable aspect is the requirement for human intervention. Already for many years, data protection laws have had an article that addresses the increased risk when decision-making takes place without human involvement. Article 22 of the GDPR, for instance, provides data subjects with the right not to be subject to fully automated decision-making that either produces legal effect or similarly significantly affects the individual. The EU AI Act goes a step further and mandates the possibility of human intervention for high-risk AI systems.

Understanding these nuances is crucial for developing an effective and compliant AI governance program that complements and enhances an existing data protection compliance program. The successful integration of AI governance into data protection programs requires a solid

understanding of both disciplines.

AI governance frameworks

Reflecting on the differences between accountable use of personal data and that of AI systems, standards institutions and (semi-)government organizations have been drafting AI governance frameworks. While many of them are intended to assist policymakers, they can also be used to shape the AI compliance efforts of individual organizations.

The following AI governance frameworks are frequently referenced:

- OECD AI Principles: The Organisation for Economic Co-operation and Development (OECD) has outlined principles for trustworthy AI, guiding companies in developing trustworthy AI and providing policymakers with recommendations for effective AI policies.
- NIST AI Risk Management Framework: The U.S. National Institute of Standards and Technology (NIST) provides a framework for better managing risks to individuals, organizations, and society associated with AI.
- IEEE Ethically Aligned Design: The Institute of Electrical and Electronics Engineers (IEEE) offers an Ethically Aligned Design (EAD) framework which guides the ethical design and implementation of autonomous and intelligent systems. The document aims to stimulate public discussion about the ethical and social implications of AI systems.
- EU Ethics Guidelines for Trustworthy AI: The EU has published guidelines on developing trustworthy AI. The focus of this document is on fostering and securing ethical and robust AI.

Interestingly, the principles in these AI governance frameworks align well with the Accountability Wheel discussed earlier. Similarities include the importance of leadership buy-in, establishing policies and procedures, and implementing risk mitigation measures. The importance of AI training is also present, which makes sense because it is even a legal requirement; any organization subject to the EU AI Act, developing or deploying AI systems, must provide AI literacy training by law.

A noticeable difference between the GDPR and the EU AI Act lies in how transparency is used to build trust. While transparency obligations for data protection purposes are legally limited to data subjects, the AI governance frameworks emphasize transparency with a wider range of stakeholders. Communicating the AI system's capabilities and limitations, as well as research and design processes, fosters better understanding and trust with business partners and B2B clients. Interestingly, the earlier introduced Accountability Wheel's transparency element suggests information to be given not only to data subjects but also to all stakeholders, going beyond, for instance, the GDPR.

Given the differences between data protection and AI governance, the question arises: can existing data protection frameworks support AI governance? Recent evidence suggests that the Accountability Wheel, for example, effectively serves as an AI compliance framework. Best practices for responsible AI from diverse sectors and regions align seamlessly with the framework's seven core elements. See CIPL's 'Building Accountable AI Programs: Mapping Emerging Best Practices to the CIPL Accountability Framework' for more.

Trade associations as resources for developing compliance programs

In addition to broader compliance frameworks, industry-specific guidance from trade associations provides valuable resources for developing governance programs. Trade associations are particularly useful for SMEs lacking resources to develop bespoke compliance programs. Resources made available by these bodies are tailored to the unique challenges and AI applications frequently used within each sector, making them more practical and accessible. For example, the Federation of European Data and Marketing (FEDMA)'s Ethical AI-Powered Marketing Charter has 'positive consumer experience,' a crucial aspect for marketers optimizing customer journeys, as a point of consideration when ensuring human centricity of AI systems. In addition, FEDMA helps its members by providing marketing and advertising services companies with a template AI policy, easily adaptable to individual company needs. Trade associations on a national level can also provide useful compliance and policy documents that reflect the context of individual countries. For example, members of the UK marketing and advertising trade association Data and Marketing Association (UK DMA) have access to updated privacy policy templates, DPIA templates, advertising risk assessment templates, and even model data processing agreements, specifically tailored to the UK marketing and advertising companies.

Beyond compliance programs

Equipped with appropriate frameworks, CPOs and DPOs can build effective compliance programs. However, it is vital to recognize that implementing these programs inevitably transforms organizational culture. The extent of this transformation varies depending on the organization's existing culture; some will experience a dramatic shift, while others with established governance structures may see a more gradual evolution.

Organizational behavior (OB) is a discipline within the field of business and management studies that covers topics related to human dynamics in the workplace. OB literature extensively covers this cultural transition process, termed 'change management.' Successful change management begins with unwavering commitment from leadership (the C-suite) and extends to every employee. All organizations, regardless of sector (e.g., business, charity, or government), are ultimately comprised of individuals working collaboratively. Their collective perception of organizational priorities shapes the overall culture, with leadership setting the tone. This explains why leadership commitment and employee training and awareness are fundamental elements in virtually all compliance frameworks.

Therefore, robust internal communication, comprehensive training, and strong leadership support are crucial for CPOs and DPOs to successfully implement highly effective compliance programs encompassing both data protection and responsible AI. CPOs and DPOs must also be excellent communicators to play their parts effectively. The success of these programs hinges not only on the technical aspects of compliance but also on the ability to effectively manage and navigate the cultural shifts they inherently bring about.

Conclusion

Data protection compliance programs protect organizations by mitigating legal and financial risks, safeguarding reputation, and fostering a culture of ethical conduct. Popular frameworks are useful for developing data protection compliance programs. AI compliance can be integrated into existing data protection frameworks, despite innate differences. Trade associations can also provide industry and geography specific input for developing a suitable compliance program. Ultimately, success depends on effective change management, beginning with leadership buy-in and extending to comprehensive employee training and communication, empowering CPOs and DPOs to lead the process.

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

Our investment in your success

No financial ties

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

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**

Country Profile: Chile

Evolution of data protection in Chile and recent legislative updates

Jaime Urzúa W.
Associate
jurzua@alessandri.cl
Alessandri Abogados, Chile

Macarena Gatica L.
Partner
mgatica@alessandri.cl
Alessandri Abogados, Chile

Introduction

Chile has been involved in data privacy regulation in Latin America since the approval of its first privacy law in 1999. However, Law No. 19.628 on Private Life (Law No. 19.628) became outdated due to the absence of a violation catalog, an official data privacy authority, and low fines, as well as significant technological progress in the region. In response, Chile has worked to update its data protection regulatory framework, leading to the approval of Law No. 21.719 on Personal Data Protection (Law No. 21.719) in December 2024, which will come into effect on December 1, 2026.

Law No 19.628 and Law No. 21.719

Law No. 19.628 was the first data privacy regulation in Chile. In 2017, the Government introduced Bill No. 11144-07 to amend the Law, based on the standards of the EU General Data Protection Regulation (GDPR), and to create a data protection agency. This bill was approved by the National Congress in August 2024, and became Law No. 21.719.

Key acts, regulations, and directives

Law No. 19.628 currently regulates data privacy in Chile but will be replaced by Law No. 21.719 in 2026. This new law introduces several significant changes, including the creation of the Agency for the Protection of Personal Data, which will be responsible for overseeing and enforcing the law.

Scope of application

Law No. 21.719 will apply to all public and private organizations that process personal data of identified or identifiable natural persons in Chile. This includes personal, sensitive, biometric, georeferenced, and minors' data, among others.

Data protection authority

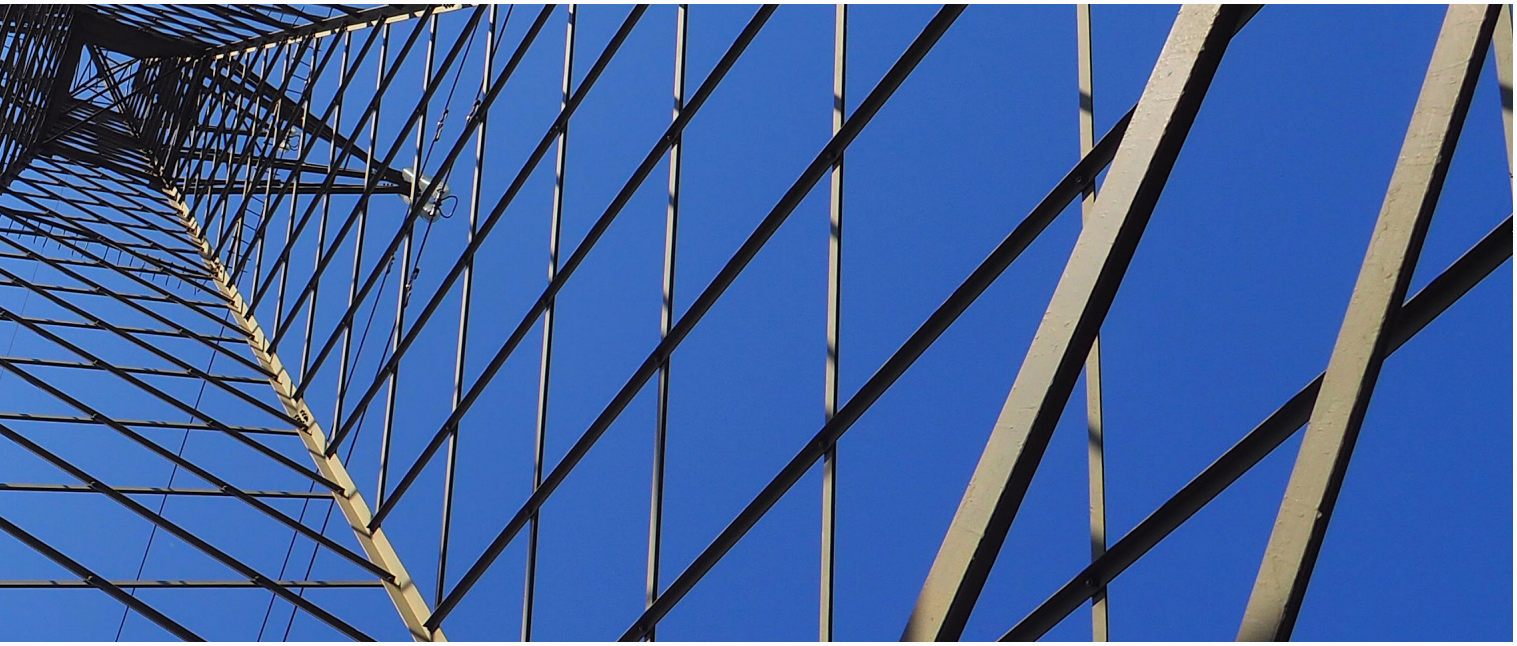
Currently, there is no specific data protection authority in Chile. The new law will create the Personal Data Protection Agency (the Agency), which will have regulatory, supervisory, sanctioning, and coordinating powers to ensure compliance with Law No. 21.719.

Legal bases for data processing

The new law establishes several legal bases for data processing, including consent, the execution of a contract, compliance with legal obligations, and the legitimate interests of the data controller.

Data subject rights

Law No. 21.719 grants data subjects a series of rights, including the right to access, rectification, deletion, opposition, data blocking, and data portability, as well as the right to object and to not be subject to decisions based on automated processing of their personal data, including profiling. These rights are personal, non-transferable, and non-waivable.



Obligations of data controllers and processors

The new law distinguishes between data controllers and processors and sets out their respective obligations. These include information and transparency responsibilities, implementing appropriate technical and organizational security measures, notifying data breaches, and maintaining confidentiality. Also, Law No. 21.719 sets out the obligation to adopt Privacy by Default and by Design measures.

International data transfers

International data transfers are permitted under the new law if the receiving country provides adequate levels of data protection. The Agency will determine which countries meet these requirements.

Data Protection Impact Assessments

The new law requires the conduct of Data Protection Impact Assessments (DPIAs) when data processing may result in a high risk to data subjects' rights.

Sanctions

Failure to comply with Law No. 21.719 may result in sanctions ranging from minor to serious to very serious, which may reach up to UTM 20,000 (approx. $1.5 million). In the case of a repeated offense, the Agency may impose a fine of up to three times the amount of offense committed. If the repeated offense is a serious or very serious infringement by a large company - as opposed to an SME - there is an alternative possibility of a fine of 2% or 4% of annual sales and service revenues.

Other relevant legislation

Cybersecurity Framework Law

On April 8, 2024, the Cybersecurity Framework Law No. 21.663 (CFL) was published in the Official Gazette. Except for certain chapters that became effective earlier, the CFL became fully effective on March 1, 2025.
The CFL establishes the institutional framework, principles, and general regulations to structure, regulate, and coordinate the cybersecurity actions of the State administration bodies and individuals, and sets out minimums for the prevention, containment, resolution, and response to cybersecurity incidents. It also creates attributions, obligations, and duties of public and private institutions.

- Creation of the National Cybersecurity Agency (ANCI): This agency will be responsible for regulating, supervising, and sanctioning public and private bodies that provide essential services and vital operators.
- Scope of application: The CFL applies to institutions providing essential services and operators of vital importance (OVIs). Essential services include electricity, fuel, tap water, digital infrastructure, transportation, banking, financial services, and health, among others.
- Cybersecurity obligations: Institutions must manage risks, report breaches, and comply with specific duties. OVIs have higher requirements and must report cyberattacks and cybersecurity incidents to the National CSIRT.
- Sanctions: Violations can be minor, serious, or very serious, with penalties that can reach up to UTM 40,000 (approx. $3 million).

The CFL is closely related to the protection of personal data since, in the context of the general obligation to report incidents, this law considers that an incident of significant impact shall be deemed to exist if it could interrupt the continuity of an essential service or affects the physical integrity or health of persons, as well as in the case of an impact on computer systems containing personal data. Thus, failure to report such incidents could lead to legal consequences and undermine the protection of personal data.

Fintech Law 21.521

Law No. 21.521 (the Fintech Law), published on January 4, 2023, aims to promote competition and financial inclusion through innovation and technology in financial services. The Fintech Law is closely related to the protection of personal data, as it introduces several provisions that affect how such data is handled and protected in the context of technological financial services.

- Open finance system (open banking): This system allows the exchange of financial information between financial service providers with the explicit consent of the customer. This implies that customers' personal and financial data will be shared between different entities, which requires strict data protection and security measures.
- Customer consent: The Fintech Law requires service providers to obtain the customer's prior, free, informed, express, and specific consent to access and share their information. This ensures that customers have control over their personal information and know how it will be used.
- Provider responsibilities: Financial service providers are responsible for ensuring the integrity, availability, security, and confidentiality of customers' personal information. They must comply with applicable laws and regulations, including Law No. 19.628 - and future Law No. 21.719.
- Authentication and security: The Fintech Law requires the implementation of robust authentication and security mechanisms to protect personal data during its exchange and storage. This includes cybersecurity and privacy standards that must be followed by all participating entities.
- Regulation and supervision: The Commission for the Financial Market (CMF) is the body responsible for supervising compliance with these personal data protection standards under the Fintech Law. The CMF may establish differentiated rules

depending on the relevance and risk of the participating entities.

Bill to regulate Artificial Intelligence (AI) in Chile - Bill N°16821-19 (the AI Bill)

On May 7, 2024, the President of the Republic presented to the Chamber of Deputies the AI Bill, which aims to regulate the use of AI systems in order to promote the development, use, and adoption of this technology, with the aim of fostering innovation processes while protecting the fundamental rights of individuals. The AI Bill intends to regulate the different actors of the AI ecosystem: suppliers that market or put into service AI systems in the national territory; implementers, importers, and distributors of AI systems, if they or their authorized representatives are located in the national territory; and suppliers and implementers of AI systems located abroad, if the output information of the AI system is used in Chile.

Following the line of the EU AI Act (approved by the European Commission in March 2024, which establishes the regulatory framework for AI systems in the EU), the AI Bill adopts an approach based on the level of risk of affecting fundamental rights, distinguishing four systems (unacceptable risk, high risk, limited risk, and no apparent risk). It is worth noting that the supervisory authority to ensure the enforcement of the AI Bill is the Law No. 21.719's Personal Data Protection Agency.

In particular, the Future Commission of the Chamber of Deputies is discussing and voting on the AI Bill. To date, only five of its 31 articles have been approved, despite the extreme urgency requested by the Executive.

Challenges in an intricate environment

Chile is moving towards a more robust data protection regulatory framework aligned with international standards. The implementation of Law No. 21.719 in 2026 will mark a significant milestone in the protection of data privacy in the country.

The biggest challenge to ensure the success of these new regulations will be to coordinate the actions of the various agencies, with responsibilities for personal data on the one hand, and the application of the various laws that already regulate these matters before Law No. 21.719 comes into force on the other.

International worldwide AI regulatory round-up

Sean Musch
Founder
s.musch@ai-and-partners.com
AI & Partners, Amsterdam

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

Welcome to our comprehensive review of worldwide AI regulatory developments up until October 2024. This update covers the latest updates from major jurisdictions across the world, providing insights into the evolving legal and regulatory landscape surrounding artificial intelligence (AI). In this issue, we explore key regulatory actions and guidelines, the potential impact on businesses, and associated risks.

Cross-border: UK, EU, and US joint statement on AI competition

On July 23, 2024, the competition regulators of the UK, EU, and US issued a joint statement addressing the regulatory challenges posed by generative AI (GenAI) models. The statement highlighted three major concerns: the concentration of critical AI resources, anti-competitive partnerships, and the dominance of a small number of AI companies in foundational AI models.

Impact

The joint statement underscores the regulators' intent to promote fair competition, safeguard consumer interests, and ensure the availability of diverse AI models. While these regulators are keen to stimulate innovation, they are equally focused on curbing monopolistic tendencies that could stifle smaller AI companies.

Business exposure

For companies relying on foundational models from major players, this development raises significant questions about future access to critical AI inputs. Businesses may face increased regulatory scrutiny over partnerships and resource access, particularly if their operations are dependent on exclusive deals with a few key suppliers. Firms should anticipate greater competition oversight, potentially resulting in new compliance obligations and restrictions on partnerships with large AI providers. Smaller AI developers might benefit from a more level playing field but will need to navigate potential restrictions imposed on accessing foundational technologies.

Asia: China, Hong Kong, and Singapore AI regulatory developments

China: Cyberspace Administration issues AI guidelines

On July 3, 2024, China's Cyberspace Administration released its Guidelines for the Construction of a National AI Industry. These guidelines aim to establish over 50 national and industry standards by 2026 and at least 20 international standards. Key areas of focus include machine learning, biometric recognition, and the development of large-scale AI models.

Impact

The guidelines emphasize creating technical standards for AI development while ensuring sustainable and secure AI industry growth. Additionally, the guidelines encourage the establishment of

regulatory frameworks, talent pools, and technical organizations dedicated to AI.

Business exposure

Companies operating in or with China must prepare for an increasingly stringent regulatory environment with standardized technical requirements. Businesses that do not align with these standards may find themselves shut out of key markets or hindered in gaining access to Chinese AI technologies. Foreign companies looking to engage with China's AI sector should focus on compliance with evolving local standards, which may require significant adaptation of existing products and services to meet regulatory demands.

Hong Kong: New AI data protection framework

On June 11, 2024, Hong Kong's Office of the Privacy Commissioner for Personal Data (PCPD) introduced the Artificial Intelligence: Model Personal Data Protection Framework. The framework offers best practices for businesses deploying AI systems involving personal data, though it remains non-binding.

Impact

The framework serves as a guide for businesses to ensure compliance with data protection laws when using AI. It emphasizes the importance of transparency, data minimization, and privacy protection in AI operations. Although non-binding, it indicates what regulators will prioritize in data breach investigations.

Business exposure

AI developers and users in Hong Kong should adopt the recommended practices to minimize legal risks, especially in case of a data breach. For companies handling personal data through AI systems, the framework provides a roadmap for avoiding future conflicts with regulatory authorities. While the framework is not yet enforceable, early compliance can enhance trust with customers and stakeholders.

Singapore: Model AI governance framework for GenAI

On May 30, 2024, Singapore's Government launched a new governance framework for GenAI. This Model AI Governance Framework sets out key principles for safety, transparency, and security. Recommendations include using anonymization techniques to protect privacy, developing clear transparency measures (e.g., 'food labels' for AI), and implementing monitoring mechanisms for AI incidents.

Impact

The framework encourages companies to adopt governance structures that ensure responsible AI development and deployment. It emphasizes building consumer trust by maintaining transparency and implementing processes to address potential risks associated with AI.

Business exposure

For companies operating in Singapore, this framework may soon become a *de facto* standard in AI governance. Businesses that fail to implement the recommendations may struggle to gain consumer confidence and face heightened scrutiny from regulators. Companies should consider investing in robust AI governance systems to not only protect privacy but also demonstrate a commitment to safe and ethical AI practices.

Europe: EU AI Act and other European regulatory updates EU AI Act updates

The EU AI Act officially came into effect on August 1, 2024. The most significant developments in the last quarter include the European AI Office's call for participation in drafting the first General-Purpose AI Code of Practice, the role of data protection authorities in overseeing compliance, and consultations aimed at the financial sector on AI use:

- General-Purpose AI Code of Practice: On July 30, 2024, the European AI Office launched a consultation on a code of practice for general-purpose AI providers. The code will serve as a tool for compliance with the EU AI Act's rules on AI model usage and deployment.
- Data protection authorities' role: The European Data Protection Board (EDPB) issued a statement on July 16, 2024, confirming that EU Member States must appoint national market surveillance authorities by August 2, 2025, to ensure the effective supervision of AI tools under the Act.
- Consultation for financial sector guidance: On June 18, 2024, the European Commission began a consultation to gather input on AI use cases, risks, and opportunities in the financial sector. The results will guide future sector-specific regulations.

Impact

The EU AI Act represents a pivotal moment in global AI regulation. Companies across the EU and those exporting AI-related services to the EU will need to ensure full compliance with its provisions by August 2026. In the financial sector, regulators will likely introduce additional rules, based on the feedback gathered during the consultation, to tailor AI regulation to the unique needs of the sector.

Business exposure

Businesses that operate in or sell to the EU must begin preparing for the EU AI Act's full implementation. Companies that develop general-purpose AI models should closely monitor the development of the Code of Practice to ensure compliance. Financial services firms, in particular, must prepare for new regulatory obligations specific to AI use, such as stringent requirements on risk management, transparency, and the protection of consumer interests.

EU institutions and GenAI guidelines

On June 3, 2024, the European Data Protection Supervisor (EDPS) released new guidelines for EU institutions on using generative AI systems. The guidelines emphasize adherence to data protection principles, particularly in the context of web scraping, data minimization, and transparency.

Impact

EU institutions must now carefully assess their use of generative AI systems to ensure compliance with data protection laws. Specific requirements include verifying the legality of data collection methods (such as web scraping) and minimizing the amount of data collected.

Business exposure

Businesses working with EU institutions, particularly those offering generative AI systems, will need to provide assurances about their data protection measures. Non-compliance with the new guidelines could result in penalties and lost contracts. Additionally, companies will need to review their data collection and processing practices to ensure compliance with the principles outlined by the EDPS.

ESMA guidance for firms using AI in investment services

The European Securities and Markets Authority (ESMA) published initial guidance on May 30, 2024, for investment firms utilizing AI in services to retail clients. ESMA's guidance emphasizes compliance with the Market in Financial Instruments Directive (Directive (EU) 2014/65) (MiFID II), particularly regarding organizational structure, client interests, and risk management.

Impact

Investment firms must ensure that their AI systems comply with MiFID II, focusing on transparency, fraud detection, risk management, and customer service. ESMA plans to continue monitoring AI developments and could introduce further regulations if necessary.

Business exposure

Firms using AI in investment services must align their systems with ESMA's expectations to avoid regulatory breaches. Companies that fail to meet MiFID II standards when deploying AI systems risk fines and reputational damage. Investment firms should review their AI strategies and governance frameworks to ensure that they prioritize client protection and regulatory compliance.

Middle East: UAE AI Charter

On July 30, 2024, the UAE launched its AI Charter through the Artificial Intelligence, Digital Economy, and Remote Work Applications Office. The charter lays out principles for safe AI development, focusing on fairness, transparency, and compliance with local and international laws.

Impact

The charter aims to create a robust regulatory framework for AI applications in the UAE, encouraging businesses to adopt ethical practices while fostering innovation.

Business exposure

Businesses operating in the UAE or planning to deploy AI technologies in the region will need to comply with the principles outlined in the AI Charter. Companies should prioritize transparency, fairness, and legal compliance in their AI operations. This may necessitate investments in ethical AI practices and audits to ensure ongoing adherence to local regulations.

UK: AI Bill and Opportunities Action Plan

AI Opportunities Action Plan

On July 26, 2024, the UK Government released its AI Opportunities Action Plan, outlining its strategic vision for the country's AI development. The plan emphasizes improving public services through AI and preparing infrastructure for the upcoming AI Bill.

Impact

The action plan will serve as a guide for the UK's future AI policies. It also outlines the Government's ambition to make the UK a global AI leader by investing in AI research, infrastructure, and skills.

Business exposure

Companies that want to capitalize on the UK's AI initiatives should align with the strategic goals outlined in the action plan. This includes staying ahead of potential regulatory changes while positioning themselves to benefit from Government-backed AI research and innovation programs. Firms should also evaluate how the UK's forthcoming AI Bill may impact their operations and adjust accordingly.

Introduction of the AI Bill

During the King's speech on July 17, 2024, the Labour Government confirmed plans to introduce new legislation governing AI technologies. The AI Bill will establish a comprehensive regulatory framework aimed at ensuring the responsible and safe development of AI.

Impact

The forthcoming AI Bill will be a critical piece of legislation shaping the UK's AI landscape. While details are still emerging, the bill is expected to impose significant requirements on AI developers, including mandatory risk assessments, transparency obligations, and ethical guidelines for AI applications.

Business exposure

Companies that develop or use AI technologies in the UK should closely follow developments around the AI Bill. Businesses will need to invest in compliance measures, such as risk management systems and reporting processes. Firms that prepare early for these changes can avoid costly disruptions and maintain their competitive edge in the evolving regulatory environment.

US: AI Regulation and the Deepfake Bill Deepfake Bill

On July 11, 2024, the Content Origin Protection and Integrity from Edited and Deepfaked Media Act (COPIED) was introduced to the U.S. Senate. This bill proposes voluntary standards for detecting and labeling deepfake content, including digital watermarks and content provenance tools to ensure authenticity.

Impact

The Deepfake Bill reflects growing concerns about the malicious use of AI to manipulate digital content. If passed, the bill will provide legal incentives for companies to implement technology capable of identifying and tracking the origin of synthetic media.

Business exposure

Media and technology companies, particularly those involved in content creation and distribution, should prepare for a future in which deepfake detection becomes a regulatory requirement. Firms will need to adopt advanced tools to ensure content authenticity and protect against reputational damage resulting from the spread of deepfake media. For companies developing deepfake technology, increased scrutiny and restrictions could lead to new legal challenges.

AI in financial services: Treasury RFI

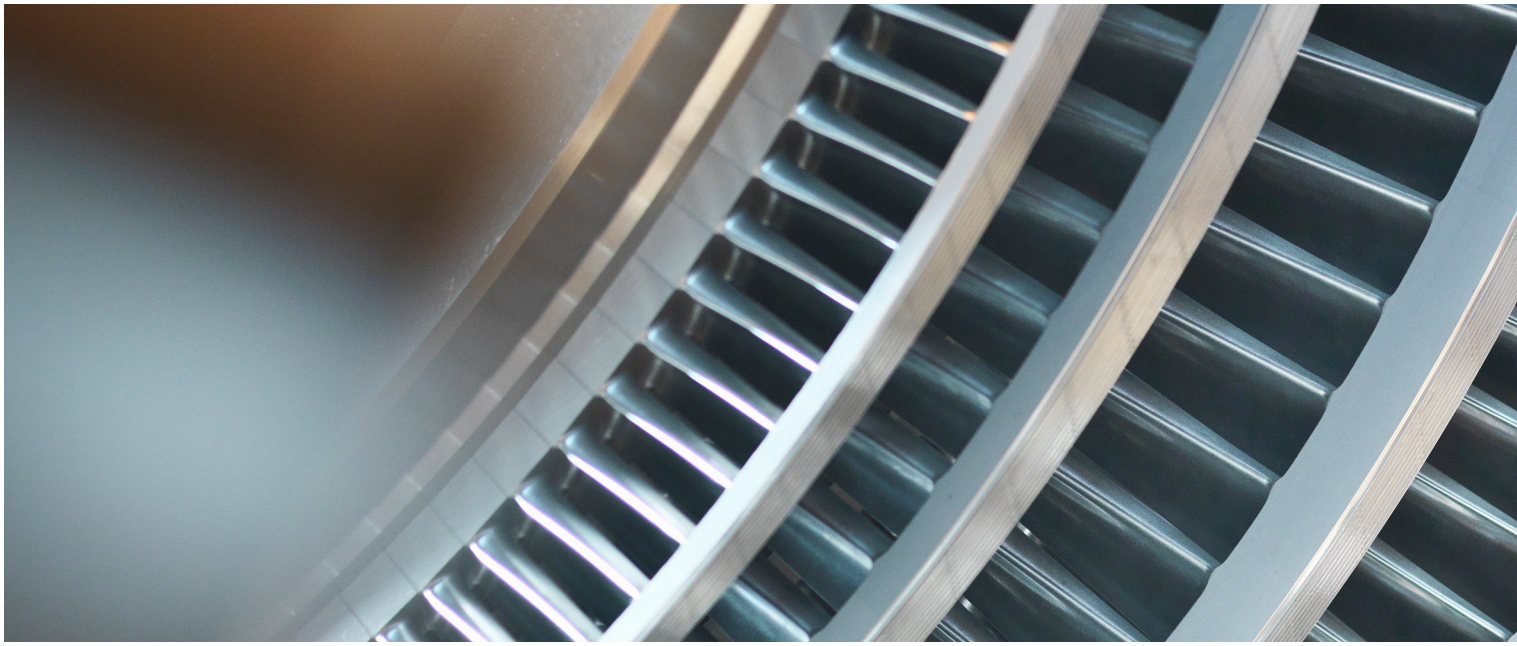
On June 6, 2024, the U.S. Department of the Treasury issued a Request for Information (RFI) to gather industry insights on the use of AI in financial services. The RFI focuses on understanding the risks, opportunities, and challenges that AI poses for the sector, including its impact on fraud detection, algorithmic trading, and customer service.

Impact

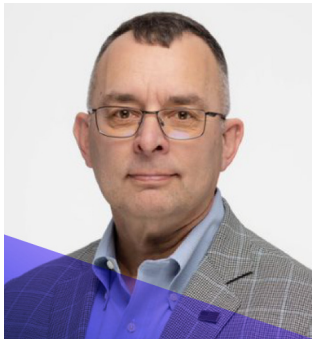
The RFI signals that the Treasury is taking a proactive approach to understanding AI's role in financial services. The results will likely inform future regulatory actions aimed at mitigating risks while promoting innovation in the sector.

Business exposure

Financial services firms using AI should anticipate new regulations that will require enhanced transparency, accountability, and risk management. Companies should review their AI systems to ensure compliance with potential future rules, particularly in areas such as fraud detection and algorithmic decision-making. Early adoption of best practices could give firms a competitive advantage while ensuring alignment with future regulations.



Meet a CPO: Hugo Teufel III



Hugo Teufel III
Vice President, Deputy General Counsel, Chief Privacy Officer
Lumen Technologies, USA

Hugo leads a team responsible for Lumen's global privacy and records management programs, as well as the provision of cybersecurity legal advice and counsel to the company. In addition, he serves on Lumen's Data & AI Steering Committee. Hugo brings more than 20 years of experience, centering on the changing landscape of privacy and security across a variety of sectors. He previously served in several leadership roles, including as Chief Privacy Counsel for Raytheon Company and as Chief Privacy Officer at the U.S. Department of Homeland Security. Hugo also served as a Judge Advocate in the Army National Guard for over 12 years.

Hugo has a B.A. in Economics with a minor in German from the Metropolitan State University of Denver, a J.D. from the Washington College of Law at American University, and an M.A. in National Security and Strategic Studies from the U.S. Naval War College. He also holds CIPP/G, CIPP/US, and CIPM certifications from the International Association of Privacy Professionals and Certificates in Privacy Engineering from Carnegie Mellon University, Strategic AI from the University of Colorado, Colorado Springs, and AI Strategy from Cornell University. Hugo is a member of the Colorado bar.

How did you first get started in privacy and data protection?

I was working in the Federal Government and my team of attorneys had responsibility for the Privacy Act and the Freedom of Information Act. Later on, I was asked a couple of times to serve as the Privacy Officer for Department of Homeland Security (DHS). I said yes the second time.

You've held several Government positions in the past, including acting as the Chief Privacy Officer for the Department of Homeland Security. How has your work compared in the field from the public to the private sector?

Working in Government, especially as the Chief Privacy Officer of the DHS, one has a greater involvement with policy issues. As well as this, the stakeholders with whom one comes into contact are different. In addition to businesses and business groups, I interacted with the various US-based privacy groups, members of Congress and their staff, international public interest groups focused on privacy and civil liberties, parliament members from various countries, members of the European Parliament, various Justice and Interior ministry officials, members of the European Commission and their staff, and

various data protection authorities and their staff. In the private sector, one is focused on compliance and staying out of the public eye.

How have you approached the design and build of privacy programs across your roles? What elements have you seen that have been the most successful?

I can't recommend the International Association of Privacy Professionals (IAPP) CIPM certification or the Privacy Program Management book enough. It's all about the fundamentals. For privacy, you need a framework upon which to build your program and then you need an inventory of the assets that process personal information (PI) and an inventory of the processing activities. The heart of the program is that data inventory, without which you know little and cannot speak to what the company is doing with personal information. Everything builds off of these two things.

As part of your current role, you act as the CPO but are also responsible for providing advice to the business on cybersecurity and artificial intelligence-related issues. How do you manage a cross-domain program, and what tips would you have for others aiming to take a holistic approach to their compliance programs?

I've never thought about 'cross-domain' programs or 'holistic approaches,' I just do the work! Seriously, there is overlap among privacy, cyber, AI, and records management - all of which fall under my team from a legal standpoint, if not operational. Each area starts with a framework and an understanding of what we're doing and why. Risk management is important. You have to align the risk with the company's appetite for risk. It's the fundamentals.

Artificial intelligence has been one of the biggest discussion topics over the last couple of years. What have been some of the key items that you've prioritized as part of an AI governance program?

The fundamentals! What are the AI use cases, what is our framework, what are the risks from the use cases, and how have we mitigated them. It's always the fundamentals.

What do you think still lies ahead for AI and compliance for organizations?

Well, there is a lot we don't know and understand about AI, which means that the risk from AI is itself not fully understood. Additionally, we need clarity over who will regulate.

What has been one of the most exciting projects you've worked on in your career and what has been the biggest challenge you've faced?

There are a lot, but I'm always hesitant to talk specifics about prior projects. That said, working on the Comprehensive National Cybersecurity Initiative (CNCI) was pretty exciting and I was able to overcome some challenges when working on behalf of the Department and the Administration. Coordinating discussions with the various privacy groups and being transparent about what we were doing made a difference in the public rollout.

What are you most looking forward to for the future of the profession and landscape?

Corporate recognition of the importance of privacy in the same way that corporations now appreciate the importance of security.

5 minutes with… Dr. Jessica Jacobi

Dr. Jessica Jacobi
Partner
jessica.jacobi@kliemt.de
KLIEMT.Arbeitsrecht, Berlin

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

I co-founded the Berlin office of KLIEMT. Arbeitsrecht (HR Lawyers) more than 20 years ago. I have a special interest in employee data protection. In the early years of my career at KLIEMT, I have had three children. I have never stopped working but my practice was smaller than it is now. I made use of the Covid imposed lockdown to train for the IAPP exam as a Certified Privacy Professional/Europe, something which I really enjoyed.

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

I would have loved to be a veterinarian; I am a huge fan of animals in general, and horses and dogs in particular. However, it is my suspicion that in the long run, I would have missed reading as much as I can and must do now, being a lawyer.

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

I love that in employment and in data protection law, there is ongoing change and development. These are really very quickly evolving areas of law. Regarding data protection law, I especially like that it is a very international area of law, with all European countries applying the same regulation. What do I find challenging? I am not a huge fan of long drawn negotiations or litigation, but in order to come to a settlement, it takes two to tango, as they say.

Where is your favorite place on earth?

Can I have several? I really love living in Berlin. I also love the Bavarian mountains where I spend a lot of time with my family, and I love California. Plus, I am happy whenever I am on top of a horse.

Who would play you in a film about your life?

If my life was worth making a movie about it, I would love to be played by Reese Witherspoon.

What is your favorite book?

I have so many! I read about two or three books per month. Mostly in English, recently also in Spanish and not so much in German. The book I would most recommend for reading is by Oliver Burkeman, '4000 weeks. Time Management for Mortals.'

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

I think being a lawyer is a great choice, it is so diverse, you can do virtually everything with this education. For someone young and new in the legal industry of law firms, I would recommend starting in a mid-size to larger law firm where you get an overview of many legal areas, even if you are specialized in your own area already. Larger firms also tend to give you better training in the formalities of being a lawyer. I would also strongly recommend trying to spend some time in other countries as a young lawyer, on secondment or as part of the legal training.

Who is your inspiration?

Actually, some of my partners. They are a hardworking and accomplished bunch of lawyers. Also, lawyers fighting for their ethical convictions, like Ruth Bader Ginsberg. And some older lawyers, managers, or politicians who really stay on top of things, experimenting with AI or publishing until they are about 100 years old, like the recently passed Henry Kissinger.

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