GIBSON DUNN

International Cybersecurity and Data Privacy Review and Outlook – 2024

Client Alert | February 16, 2024

For the sixth consecutive year, and following the publication of Gibson Dunn's annual U.S. Cybersecurity and Data Privacy Outlook and Review in 2024, we offer this separate International Outlook and Review. As every year, this Outlook and Review provides an overview of past and upcoming developments related to global privacy and cybersecurity laws. In 2023, data protection laws continued to be adopted across numerous international jurisdictions. Switzerland, the United Kingdom, India, Vietnam and Saudi Arabia, among others, passed new laws, amendments or implementing regulations paving the way for a new round of significant data privacy regimes. It is expected that authorities will make full use of their powers in order to apply and enforce their respective data protection legislation in the near future. In the European Union ("**EU**"), EU supervisory authorities continued to apply and enforce the General Data Protection Regulation ("**GDPR**") vigorously while the European Data Protection Board ("**EDPB**") issued and updated various guidelines providing useful interpretation of the GDPR. Finally, we noted a significant number of developments in the European digital regulatory landscape. We cover these topics and many more in this year's International Cybersecurity and Data Privacy Outlook and Review. **I. European Union**

A. EU-U.S. Data Privacy Framework

As we indicated in the 2023 International Outlook and Review, the EU-U.S. Privacy Shield was struck down on 16 July 2020, by the ***Schrems II* ruling** of the Court of Justice of the European Union ("**CJEU**").[1] In order to replace the Privacy Shield and to safeguard cross-border data flows, the European Commission had launched the process to adopt an adequacy decision for the transfer of personal data between the EU and the U.S. (the "**EU-U.S. Data Privacy Framework**"). On 10 July 2023, the European Commission adopted its adequacy decision for the EU-U.S. Data Privacy Framework. This decision concludes that the United States ensures an adequate level of protection – comparable to that of the EU – for personal data transferred from the EU to U.S. companies under the new framework. The EU-U.S. Data Privacy Framework introduces new binding safeguards to address all the concerns raised by the CJEU, including limiting access to EU data by U.S. intelligence services to what is necessary and proportionate, and establishing a Data Protection Review Court ("**DPRC**"), to which EU individuals will have access. U.S. companies are able to join the EU-U.S. Data Privacy Framework by committing to comply with a detailed set of privacy obligations.

B. Network Information Security Directive

The Directive (EU) on measures for a high common level of cybersecurity across the Union 2022/2555[2] ("**NIS 2 Directive**") entered into force on 16 January 2023 and replaced the Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union ("**Network Information Security**" or "**NIS**"). The NIS 2 Directive sets the baseline for cybersecurity risk management measures, and reporting obligations across all sectors that are covered by the Directive, such as energy, transport, health and digital infrastructure (e.g., cloud computing service providers, data center service providers, providers of public electronic communications networks or services) and digital providers (e.g., providers of online marketplaces, providers of social networking services platforms). In addition, the NIS 2

Related People

Ahmed Baladi

Vera Lukic

Joel Harrison

Connell O'Neill

Clémence Pugnet

Thomas Baculard

Hermine Hubert

Sarah Villani

Anastasia Katsari

Nick Hay

QX Toh

Directive sets the baseline for reporting obligations. In particular, if an incident has a significant impact on the provision of services covered by the Directive, an authority must be notified without undue delay. The Member States will have to adopt and publish the measures necessary to comply with the NIS 2 Directive by 17 October 2024.[3]

C. Data Governance Act

The Regulation (EU) 2022/868 on European data governance of 30 May 2022 ("**Data Governance Act**")[4], entered into force on 24 September 2023. The Regulation seeks to increase trust in data sharing, strengthen mechanisms to increase data availability and overcome technical obstacles to the reuse of data, notably with public actors. In particular, the Data Governance Act allows new data intermediaries to act as trustworthy actors in the data economy and lays down rules to enable data altruism.

D. The Digital Operational Resilience Act

The Regulation (EU) 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector, ("**Digital Operational Resilience Act**" or "**DORA**"),[5] which focuses on preventing and mitigating cyber threats, entered into force on 16 January 2023 and will apply from 17 January 2025 to financial entities (including credit and payment institutions, electronic money institutions, crypto-asset service providers), as well as information and communication technology ("**ICT**") third-party service providers. In particular, financial entities' management body will be responsible to define, approve and oversee the management of ICT risks. Financial entities will also have requirements on reporting major ICT-related incidents to the competent authorities. In addition, DORA contains requirements in relation to the contractual arrangements concluded between ICT third-party service providers and financial entities.

E. Data Act

On 22 December 2023, the Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data[6] was published in the Official Journal of the European Union. Most of the provisions of the Data Act will be applicable on 12 September 2025 but some will be applicable from 12 September 2026 and 12 September 2027. Among the key measures of the Data Act, the Regulation imposes obligations on manufacturers and service providers to let their users (companies or individuals) access and reuse the data generated by the use of their products or related services. In addition, the Data Act aims at easing the sharing of user data to third parties and the switching between providers (portability). Finally, the Regulation prohibits unfair contractual terms in data sharing.

F. Cyber Resilience Act

The proposal for a Regulation on cybersecurity requirements for products with digital elements of 15 September 2022 ("**Cyber Resilience Act**" Proposal) aims at protecting both consumers and businesses from products with inadequate security features and thereby ensure a better level of cybersecurity. In particular, the Proposal introduces mandatory cybersecurity requirements and obligations for manufacturers as well as importers and distributors of products with digital elements within the EU. Any vulnerability contained in the product or any incident impacting its security will have to be reported by the manufacturer to the EU Agency for Cybersecurity ("**ENISA**"). The "critical products" (e.g., operating systems, firewalls or network interfaces) would be subject to a specific compliance procedure. This Proposal, if adopted, will be directly applicable in all Member States. Sanctions for violation will depend on the concerned breach (up to €15 million or 2.5% of the company's total worldwide annual turnover of the preceding financial year, whichever is higher). On 30 November 2023, the Council and the European Parliament reached a provisional agreement on the proposed Regulation. The agreement reached is now subject to formal approval by both the European Parliament and the Council. Once adopted, companies will have two years to adapt to the new requirements.

G. EDPB Guidance

The EDPB updated its existing guidelines on various topics, including: i. **Guidelines 04/2022 on the calculation of administrative fines under the GDPR**,[7] which aim to provide a clear and transparent basis for the supervisory authorities' setting of fines. ii. **Guidelines 03/2021 on the application of Article 65(1)(a) GDPR**,[8] which aim to clarify the applicable legal framework and main stages of the procedure, in accordance with the relevant provisions of the Charter of Fundamental Rights of the European Union, the GDPR and EDPB Rules of Procedure. iii. **Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement**,[9] which aim to inform about certain properties of facial recognition technology and the applicable legal framework in the context of law enforcement (in particular the Law Enforcement Directive). iv. **Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority**,[10] which aim to update the previous version of these guidelines since there was a need for further clarifications, specifically regarding the notion of main establishment in the context of joint controllership and taking into account the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR. v. **Guidelines 01/2022 on data subject rights – Right of access**,[11] which aim to provide guidance on how the right of access has to be implemented in practice. vi. **Guidelines 9/2022 on personal data breach notification under the GDPR**,[12] which aim to update the previous version of these guidelines since there was a need to clarify the notification requirements concerning personal data breaches in non-EU establishments. vii. **Guidelines 07/2022 on certification as a tool for transfer**,[13] which aim to provide guidance as to the application of Article 46 (2) (f) of the GDPR on transfers of personal data to third countries or to international organisations on the basis of certification. viii. **Guidelines 05/2021 on the interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR**,[14] which aim to clarify the scenarios for which the EDPB considers that the requirements of Chapter V should be applied. To that end, the EDPB has identified three cumulative criteria to qualify a processing operation as a transfer. ix. **Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them**,[15] which aim to offer practical recommendations to social media providers as controllers of social media, designers and users of social media platforms on how to assess and avoid so-called "deceptive design patterns" in social media interfaces that infringe on GDPR requirements. The EDPB also issued guidelines for public consultation, including: i. **Guidelines 2/2023 on Technical scope of Article 5(3) of ePrivacy Directive[16]** which aim at conducting a technical analysis on the scope of application of Article 5(3) ePrivacy Directive, namely to clarify what is covered by the phrase 'to store information or to gain access to information stored in the terminal equipment of a subscriber or user'. ii. **Guidelines 01/2023 on Article 37 Law Enforcement Directive**[17], which aim at providing guidance as to the application of Article 37 of the Law Enforcement Directive on transfers of personal data by competent authorities of EU Member States to third country authorities or international organisations competent in the field of law enforcement. **II. Enforcement by Supervisory Authorities**

In 2023, the GDPR and the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ("**e-Privacy Directive**")[18] continued to be applied and enforced by Member States' supervisory authorities which imposed substantial fines. We have gathered below a list of important fines published in 2023:

- On 15 June 2023, the French Supervisory Authority imposed a €40 million fine on a global adtech giant for a multitude of GDPR violations related to its targeted advertising practices.[19] The company specializes in "behavioural retargeting", which consists of tracking the navigation of Internet users in order to display personalized advertisements. In particular, the Authority considered that the advertising company had failed to demonstrate that the data subjects gave their consent.
- On 28 September 2023, the Italian Supervisory Authority imposed a fine of €10

million on an electricity and gas supplier, for the activation of unsolicited contracts in the free market through the processing of inaccurate and out-of-date customer data.[20] The Authority also ordered corrective actions, such as implementing a contract accuracy verification system, alert systems to identify improper data acquisition, and enhancing audit procedures against sales agencies.

- On 13 April 2023, the Italian Supervisory Authority fined a telecommunications giant €7.6 million for unlawful processing of millions of individuals' data for marketing purposes (namely calls without any consent or in spite of the called individuals being on a public opt-out register).[21]
- On 5 October 2023, the Croatian Supervisory Authority fined a debt collection company €5.47 million for lack of appropriate technical measures to protect personal data, lack of legal basis and failure to inform data subjects about the processing of their health data and telephone records.[22]
- The French Supervisory Authority published a decision issued on 17 April 2023, imposing a €5,2 million fine on a facial recognition company, for failing to comply with the injunction issued in its October 2022 sanction decision. Back in October 2022, the Authority had fined the company €20 million and enjoined the company to refrain from collecting and processing the data of individuals in France without a legal basis, and to delete the data of these individuals after responding to requests for access. The injunction was accompanied by a penalty of 100,000 euros per day of delay at the end of the two-month period. The Authority considered that the company had not complied with the order and imposed an overdue penalty payment[23].
- On 12 June 2023, the Swedish Supervisory Authority imposed a SEK58 million fine (approx. €4,9 million) fine on a company providing an audio streaming service for shortcomings regarding the right of access.[24] The Authority considered that the company does not provide information about how it uses the personal data upon a request of access of individuals and specifies that this information must be easy to understand. In addition, personal data that is difficult to understand, such as those of a technical nature, may need to be explained not only in English but in the individual's own native language. The Authority has further found that the company had failed in its handling of requests for access related to two out of three of the complaints examined.
- On 28 August 2023, the Swedish Supervisory Authority fined an insurer SEK35 million (approx. €3 million) for exposing on its online portal sensitive data belonging to hundreds of thousands of customers.[25]
- On 28 July 2023, the Spanish Data Supervisory Authority issued a €2,5 million fine on a banking institution for not complying with the data protection by design and by default requirements and for not implementing appropriate security measures to address potential risks.[26]
- On 4 May 2023, the Croatian Supervisory Authority imposed a €2.26 million fine on a debt collection agency. The investigation revealed three violations of the GDPR, namely failure to inform data subjects about data processing activities, failure to have a data processing agreement with a processor and failure to implement appropriate technical and organisational measures.[27]
- On 27 November 2023, the Norwegian Supervisory Authority announced a NOK20 million (approx. €1.7 million) fine issued to the Norwegian public welfare agency because the safeguarding of confidentiality in the IT systems of the agency was unsatisfactory.[28]
- On 27 June 2023, the Swedish Supervisory Authority fined a mass media company SEK13 million (approx. €1 million) for profiling customers and website visitors without consent (unlawfully trying to rely on legitimate interest).[29]
- On 22 June 2023, the Italian Supervisory Authority announced that a company in

the motorway business was fined €1 million for violating the GDPR. In this ruling, the Authority considered that the company violated the principles of accuracy and transparency, given the failure to provide adequate information in relation to the processing, as well as the misclassification of the GDPR status.[30]

III. Developments in Other European Jurisdictions: UK, Switzerland and Turkey

A. UK 1. Online Safety Act

The Online Safety Bill received Royal Assent on 26 October 2023, becoming the Online Safety Act 2023. The Act introduces new obligations on the design, operation and moderation of platforms. The UK Office of Communications ("**Ofcom**") will enforce the Act's requirements on platforms and will release its plan to implement online safety laws into practice in the following three phases[31]: (i) illegal content; (ii) child safety, pornography, and protecting women and girls; and (iii) additional duties for categorised services. On 9 November 2023, Ofcom released its first guidance and draft code of practice under the Act that covers illegal content such as terrorism and child abuse material. Ofcom is currently "consulting on these detailed documents, hearing from industry and a range of experts as [Ofcom] develop[s] long-term, final versions that [Ofcom] intend[s] to publish in autumn [2024]"[32]. Responses to the consultation can be submitted until 23 February 2024.[33]

2. Data Protection and Digital Information Bill No.2

The Data Protection and Digital Information Bill was first introduced in July 2022 and paused in September 2022 so that ministers could engage in a co-design process with business leaders and data experts.[34] The Data Protection and Digital Information (No. 2) Bill[35] (the "**DPDI Bill**") was introduced on 8 March 2023 and aims to introduce a business-friendly framework[36], cut down paperwork for businesses and reduce unnecessary cookie pop-ups. The Information Commissioner's Office (the "**ICO**") responded to the DPDI Bill in May 2023, setting out general comments (such as welcoming the UK Government's decisions that maintain the ICO's high standards for the protection of individuals' rights and freedoms), as well as targeted comments on specific clauses of the DPDI Bill.[37] The DPDI Bill is currently at the Committee stage in the House of Lords.

3. UK-U.S. Data Bridge

On September 21, 2023 the UK Secretary of State for Science, Innovation and Technology laid regulations in the UK Parliament to give effect to the decision to establish a UK-U.S. Data Bridge. The decision was based on her determination that the UK-U.S. Data Bridge "maintains high standards of privacy for UK personal data"[38]. The UK-U.S. Data Bridge came into effect on 12 October 2023 and permits organizations in the UK to transfer personal data to U.S. organizations certified to the "UK Extension to the EU-U.S. Data Privacy Framework" without the need for further safeguards, such as international data transfer agreements (the UK version of the EU's standard contractual clauses). There are requirements for both UK and U.S. organizations in order to implement the Data Bridge, such as updating privacy policies and certifying to the Data Privacy Framework List[39].

4. AI and Data Protection

On 15 March 2023, the ICO announced that it had updated its guidance on artificial intelligence ("**AI**") and data protection.[40] The ICO provides detailed guidance on how to apply the principles of the UK GDPR. The ICO indicates that the changes respond to requests from UK industry to clarify requirements for fairness in AI, and provides updated guidance in the areas of accountability and governance, transparency, lawfulness, accuracy, and fairness. The ICO also provides a toolkit regarding AI and data protection (that is designed to provide practical support to reduce risks to individuals' rights and

freedoms caused by an organisation's own AI systems)[41] and a data analytics toolkit (to assist organisations to recognise the rights and freedoms of individuals created by the use of data analytics)[42].

5. Data Scraping

On 24 August 2023, the ICO released a joint statement on data scraping and the protection of privacy with data protection and privacy authorities from Australia, Canada, Hong Kong, Switzerland, Norway, New Zealand, Columbia, Jersey, Morocco, Argentina and Mexico.[43] The statement calls for the protection of people's personal data from unlawful data scraping taking place on social media sites. It also sets expectations for how social media companies should protect individuals' data from unlawful data scraping.

6. Direct Marketing and Regulatory Communications Guidance for Regulated Private Companies

In March 2023, the ICO issued guidance to businesses operating in regulated private sectors (i.e., "sectors where a statutory regulator has oversight"[44] such as the finance, pension, communications and energy sectors) on direct marketing and regulatory communications. The guidance aims to help businesses identify when a regulatory communication message might count as direct marketing. It also covers what businesses need to do to comply with data protection and ePrivacy law in sending messages that qualify as direct marketing.

B. Switzerland

On 1 September 2023, the Federal Act on Data Protection 2020 ("**FADP**")[45] and the Ordinance on the Federal Act on Data Protection ("**FODP**")[46] entered into force. Following this new regulation, the Federal Data Protection and Information Commissioner ("**FDPIC**") introduced a "DataBreach Portal" designed for reporting security vulnerabilities, an online registration system for the contact details of DPOs and a portal for Federal bodies to report their data processing activities to the FDPIC.[47] On 4 April 2023, the FDPIC issued a statement on the use of ChatGPT and comparable artificial intelligence supported apps. In particular, the FDPIC recognised the opportunities of using AI-supported applications such as ChatGPT for society and the economy. However, it emphasises that the processing of personal data using these new technologies also entails risks for privacy and informational self-determination.[48] In Switzerland, the Federal Administration is evaluating various approaches to regulating AI by the end of 2024. Finally, the Swiss-U.S. Data Privacy Framework ("**Swiss-U.S. DPF**") was adopted in July 2023 so that participating US organisations will be deemed to provide adequate privacy protection as required for receiving personal data from Switzerland under the FADP. However; to date, personal data from Switzerland cannot be transferred to U.S. organisations in reliance on the Swiss-U.S. DPF until the Swiss Federal Administration issues an adequacy decision recognizing that the Swiss-U.S. DPF ensures data protection consistent with Swiss law. **C. Turkey** On 13 October 2023, the Personal Data Protection Authority ("**KVKK**") published guidelines on considerations in the processing of genetic data. In particular, the KVKK provides guidance for controllers to process personal data based on correct legal basis and to fulfil their obligations in accordance with the regulation.[49] On 26 October 2023, the KVKK announced that it signed a cooperation and information sharing protocol with the Competition Authority. In particular, the KVKK considered that the increasing processing of personal data through big data technologies may raise significant concerns in terms of competition and the protection of personal data, making cooperation between the relevant authorities inevitable.[50] **IV. Developments in Asia-Pacific**

A. Australia

As explained in previous editions of the International Outlook and Review, the Australian Government commenced a wholesale review of the Privacy Act 1988 ("**Privacy Act**") in

2020, with a view to implementing significant reforms to the country's privacy regime. After nearly three years and multiple rounds of consultation, the Attorney-General released the final report on 16 February 2023 ("**Privacy Act Review Report**").[51] The Government subsequently considered the Privacy Act Review Report and released its proposed response on 28 September 2023.[52] The Privacy Act Review Report puts forward 116 proposals, aimed at clarifying the scope of the Privacy Act, uplifting protections for individuals, providing clarity for regulated entities and enhancing enforcement mechanisms. In its response, the Government agreed to 38 of those proposals, agreed in-principle to a further 68 and noted the remaining 10. Where the Government "agreed in-principle" with a proposal, it has indicated that its agreement is subject to further engagement with industry and a comprehensive impact analysis to strike a balance between the protection of individual privacy and the resulting cost to businesses. What this means in practice remains to be seen. Key reforms that the Government has agreed or agreed in-principle to include:

- expanding the definition of personal information to include inferred or generated information, and clarifying that de-identification is a process rather than an outcome;
- introducing a new definition of sensitive information that includes genomic information, and requiring explicit consent for its collection, use and disclosure;
- strengthening the consent requirements by making consent clear, specific, informed, unambiguous, freely given and easy to withdraw;
- creating new rights for individuals, such as the right to access and correct their personal information, the right to delete their personal information, the right to data portability and the right to object to certain processing activities;
- enhancing the obligations for entities, such as requiring them to conduct privacy impact assessments for high-risk practices, to implement privacy by design and default principles and to adopt data minimisation and retention policies;
- increasing the enforcement and oversight powers of the regulator, including by enabling it to issue infringement notices, civil penalties, enforceable undertakings, injunctions and compensation orders; and
- establishing a mechanism to recognise countries and certification schemes that provide adequate or comparable protection to personal information transferred from Australia, and developing standard contractual clauses for cross-border data flows.

The Attorney-General will lead the next stage of reform required to implement the proposals in the Privacy Act Review Report, including the following:

- developing legislative proposals which are 'agreed' and conducting further targeted consultation with entities on proposals which are 'agreed in-principle' to explore whether and how they could be implemented so as to proportionately balance privacy safeguards with the corresponding regulatory burdens;
- developing a detailed impact analysis, to determine potential compliance costs for industry and other potential economic costs or benefits of the revised regime (including for consumers); and
- progressing further advice to Government in 2024, including outcomes of additional consultation and legislative proposals.

The Government has indicated that it will consider appropriate transition periods as part of the development of legislation as well as appropriate guidance and other supports which could be developed to help entities understand their compliance requirements. Legislative reforms to the Privacy Act will also be complimented by other reforms that are being progressed by the Government, including the Digital ID, the National Strategy for Identity

Resilience and Supporting Responsible AI in Australia. In this context, the Government released the 2023-2030 Australian Cyber Security Strategy and Action Plan on 22 November 2023.[53] The Strategy and Action Plan set out a vision for Australia to become a world leader in cyber security by 2030. As part of this, the Government has proposed key legislative reforms, including:

- introduction of a no-fault, no-liability ransomware reporting regime for businesses;
- amendments to the existing data retention requirements in Australia, with a focus on non-personal data;
- amendments to the *Security of Critical Infrastructure Act 2018* (Cth) to extend its application to data storage systems and business critical data, increase Government management, review and remedy powers and impose more onerous cyber obligations and reporting requirements on entities operating certain critical infrastructure;
- introduction of a limited use obligation for cyber incident information provided to the Australian Signals Directorate (ASD) and the National Cyber Security Coordinator, restricting how such information can be used by other Government entities (including regulators);
- establishment of a Cyber Incident Review Board to conduct no-fault incident reviews and share findings with the Australian public; and
- introduction of mandatory secure-by-design standards for Internet of Things (IoT) devices, a voluntary labelling scheme for consumer-grade smart devices and a voluntary code of practice for app stores and app developers.

The Government has committed $586.9 million to the Strategy. In December 2023, the Department of Home Affairs released a Consultation Paper providing further detail with respect to certain proposed legislative reforms contemplated in the Action Plan.[54] The Consultation Paper is open for public consultation and submissions will close on 1 March 2024.

B. China

China's Personal Information Protection Law ("**PIPL**") continued to take shape in 2023 as the Cyberspace Administration of China ("**CAC**") issued further implementing regulations and guidelines in both draft and final form. Notable regulations and guidelines that were issued include the following:

- ***Measures on the Standard Contract for the Export of Personal Information*** – In February 2023, the CAC released the final version of the Measures on the Standard Contract for the Export of Personal Information[55] along with the Standard Contract for the export of personal information.[56]
    - The Measures and Standard Contract supplement Article 38(3) of the PIPL and establish requirements for Chinese controllers and foreign recipients in relation to the export of personal information from China. While the new requirements came into effect on 1 June 2023, controllers had a six-month grace period (which expired on 30 November 2023) to ensure compliance.
    - Controllers are only permitted to utilise the Measures where they are not a critical information infrastructure operator ("**CIIO**") and do not otherwise meet certain volume thresholds with respect to their data processing or exports. Prior to relying on the Measures, eligible controllers must also undertake the following:
        - confirm that they are eligible to utilise the Standard Contract (i.e., do not meet the prescribed thresholds);
        - conduct and complete a personal information protection impact

assessment ("**PIPIA**");

- negotiate and execute the Standard Contract with the foreign recipient based on the template issued by the CAC; and
- file the completed PIPIA report along with the executed Standard Contract with the CAC.

- ***Guidelines for the filing of Standard Contracts for Exporting Personal Information*** – In May 2023, the CAC published new Guidelines for the filing of Standard Contracts for Exporting Personal Information.[57] These guidelines echo the filing requirements set out in the Measures described above and provide an outline of the filing process that controllers are required to undertake pursuant to the Measures.
- ***Draft Administrative Measures for Compliance Audit of Personal Information Protection*** – In August 2023, the CAC published the draft Administrative Measures for Compliance Audit of Personal Information Protection for public comment.[58] The draft Measures set out requirements for compliance audits under Articles 54 and 64 of the PIPL, which stipulate that controllers must regularly conduct compliance audits to ensure compliance with the PRC's laws and administrative regulations and otherwise authorise responsible authorities to mandate compliance audits.
- ***Draft Provisions on Regulating and Promoting Cross-Border Data Transfers*** – In October 2023, the CAC published draft Provisions on Regulating and Promoting Cross-Border Data Transfers.[59] These Provisions appear to be an attempt by CAC to reassure foreign businesses regarding compliance with the onerous data export restrictions imposed by those Measures implementing Article 38 of the PIPL.
  - The draft Provisions contemplate the following:
    - introduction of a potential waiver (exercisable by CAC) of the requirement to conduct a Security Assessment for controllers that export the personal information of more than 100,000 but less than 1 million people;
    - clarification that data will only be regarded as "important data" if it is explicitly designated as such by regulators or local authorities; and
    - exemption of specified cross-border data transfers from the transfer mechanisms set out in Article 38, including (i) for personal information that is not collected or generated within the PRC; (ii) where it is necessary for the performance of a contract to which the data subject is a party to; (iii) employee data cross-border transfers that are necessary for HR management in accordance with legally formulated labour policies or collective employment contracts; (iv) cross-border data transfers by controllers that expect to transfer the personal information of less than 10,000 individuals out of the PRC within a year; and (v) cross-border data transfers falling outside the negative list to be formulated by Free Trade Zones.
  - Public comment on the draft Provisions ended on 15 October 2023, however, the CAC has not yet issued a final version of the Provisions.
- ***Practical Guidelines on Cross-border Personal Information Protection Requirements*** – In November 2023, China's National Information Security Standardisation Technical Committee ("**TC260**") published the draft Practical Guidelines on Cross-border Personal Information Protection Requirements in the Guangdong-Hong Kong-Macau Greater Bay Area ("**Draft GBA Guidelines**").[60] The Draft GBA Guidelines propose a certification regime for cross-border data transfers within the GBA (i.e., cities in the Guangdong province and Hong Kong).

Further details and the implications of the Draft GBA Guidelines outside of China are described in the Hong Kong summary below.

C. India

After several years and multiple proposed bills, the Indian Government finally enacted a comprehensive data protection law in 2023. The Digital Personal Data Protection Act, 2023 (the "**DPDP Act**") received royal assent on 11 August 2023 and will come into force in phases (on dates to be notified), effecting wholesale changes to the processing and protection of personal data in the world's most populated country.[61] The DPDP Act represents a more streamlined and focused approach to data protection regulation than prior iterations, departing from the 2022 draft which was criticised as being overly prescriptive and compliance-heavy, and for providing undue access to data by state and law enforcement agencies. While the DPDP Act sets out a framework for India's new data protection regime, many of the details are pending the release of implementing regulations which the Government plans to finalise in due course. Key features of the DPDP Act include the following:

- ***Extraterritorial application*** – the DPDP Act will apply to processing conducted outside of India if performed in connection with offering goods or services to data subjects in India (referred to as "data principals").[62] Unlike equivalent foreign data protection regimes (such as the GDPR and CCPA), the DPDP Act does not also apply extraterritorially to processing conducted to monitor the behaviour of data subjects located in India. Further, in light of India's substantial inbound outsourcing industry, the provisions of the DPDP Act setting out the obligations of controllers (referred to as "data fiduciaries"), rights of data subjects and restrictions on data exports for processing will not apply to the processing of foreign individuals' personal data carried out in India pursuant to a contract between a controller and a person located outside of India.[63]
- ***Sensitive personal data*** – the DPDP Act does not contain any supplemental obligations with regard to the processing of specific types of data (e.g., what would be considered "special category personal data" under the GDPR or "sensitive personal information" under the CCPA). Despite this, the DPDP Act requires that controllers obtain consent from a parent or lawful guardian when processing the personal data of children (being those under the age of 18) or persons with disabilities.[64]
- ***Consent to processing*** – the DPDP Act imposes a notice and consent regime for the processing of personal data.[65] Consent must be free, specific, informed, unconditional and unambiguous, and should be given through clear affirmative action. When obtaining consent, controllers must provide a clear and plainly worded privacy notice to data subjects stating (i) the type of personal data being processed; (ii) the purpose of the processing; and (iii) how data subjects can exercise certain rights under the DPDP Act, including to withdraw their consent and file a complaint with the regulator. Consent is not required in certain prescribed circumstances, including when processing is necessary to undertake a merger or similar corporate action.
- ***Grounds for processing*** – the DPDP Act provides a limited set of legitimate grounds for processing in the absence of consent,[66] including: (i) for fulfilling any obligation under law; (ii) in order to respond to a medical emergency; and (iii) where the data subject has voluntarily provided their personal data to the controller and has not indicated an objection to the use of their personal data. Notably, the reasonable purposes and public interests grounds contained in the 2022 draft were excluded from the final version of the DPDP Act.
- ***Obligations of controllers*** – the DPDP Act imposes broad obligations on controllers,[67] including to (i) ensure processors' compliance with the act; (ii) establish a mechanism for addressing data subject complaints; (iii) ensure the

accuracy and completeness of data; and (iv) delete data if the data subject has withdrawn consent or if it is reasonable to assume that the purpose for processing is not or no longer being served. Controllers designated as "Significant Data Fiduciaries" by the Government (on the basis of factors such as the volume or sensitivity of personal data processed) are also required to (i) appoint a data protection officer and an independent data auditor; and (ii) conduct periodic audits and data protection impact assessments.[68]

- ***Cross-border transfers and data localisation*** – the DPDP Act permits cross-border transfers of personal data to any country unless specifically restricted by the Indian Government.[69] This departs from the 2022 draft, which contemplated a whitelist for this purpose. The DPDP Act also excludes data storage and localisation requirements contained in the 2022 draft that were heavily criticised by commentators and industry groups.
- ***Penalties for non-compliance and enforcement*** – the DPDP Act imposes penalties for non-compliance depending on the type and nature of breach up to a maximum of 250 crore rupees (~USD 30 million).[70] The newly formed Data Protection Board ("**DPB**") is responsible for enforcement of the DPDP Act, although its composition and functioning remains subject to the Government's release of implementing legislation.
- ***Government blocking powers*** – the DPDP Act permits the Government to block public access to a controller's platform on the recommendation of the DPB, provided that doing so is necessary or expedient in the interests of the public and the controller has had an opportunity to respond.

D. Indonesia

As explained in the 2023 International Outlook and Review, 2022 was a landmark year for data protection in Indonesia in light of the enactment of Law No.27 of 2022 on Personal Data Protection ("**PDP Law**"). While the reform agenda in 2023 was necessarily more muted, the Ministry of Communications and Informatics ("**MOCI**") publicly released the draft Government Regulation on the Implementation of the Personal Data Protection Law ("**Draft Regulation**") on 31 August 2023.[71] Public consultation on the Draft Regulation closed on 14 September 2023 and the Government is expected to release a final version prior to the PDP Law coming into effect later in October 2024. The Draft Regulation further clarifies the provisions of the PDP Law, setting out binding obligations for covered entities in order to ensure their compliance. The Draft Regulation is extensive (arguably unnecessarily so, comprising 245 articles over 180 pages), however, notable provisions include the following:

- ***Scope of personal data*** – the Draft Regulation provides the MOCI with the discretion to designate certain data as "specific personal data" if the processing of such data has the potential to have a harmful impact on data subjects, potentially widening the scope of the PDP Law in the future.
- ***PDP Agency*** – the Draft Regulation specifies the detailed responsibilities of the PDP Agency, which will supervise the implementation of the PDP Law. These responsibilities include supervising the compliance of covered entities with the PDP Law and its regulations, investigating and tracking alleged violations and imposing administrative sanctions against covered entities where violations are found to have occurred. Despite its extensive mandate, the Government has yet to formally establish the PDP Agency.
- ***Consent to processing*** – the Draft Regulation clarifies that where processing is undertaken on the basis of consent, data subjects must have been provided with a privacy notice and given their explicit lawful consent (including the consent of a parent or lawful guardian where the processing is in relation to personal data of children or persons with disabilities).

- ***Grounds for processing*** – the Draft Regulation provides that controllers intending to undertake processing of personal data on the basis of legitimate interest (as provided for in the PDP Law) must first conduct a legitimate interest assessment to assess the balance between its own interests and the rights of data subjects. Despite this, the Draft Regulation does not provide further clarification or examples as to what would constitute a "legitimate interest" for the purposes of the PDP Law.
- ***Data subject rights*** – the Draft Regulation further details the rights of data subjects contemplated in the PDP Law. The Draft Regulation also provides a short '3 x 24' hour timeframe for controllers to respond to requests by data subjects to exercise their rights.
- ***Appointment of a data protection officer (DPO)*** – the Draft Regulation requires appointment of a DPO where a controller or processor: (i) processes personal data for public service purposes; (ii) engages in core activities that involve regular and large-scale systematic monitoring of personal data; and (iii) conducts large-scale processing of personal data related to specific personal data and/or criminal offenses. Appointment of a DPO is otherwise not mandatory.
- ***Cross-border transfers*** – the Draft Regulation specifies that the PDP Agency will issue a list of countries deemed to have equal or higher levels of personal data protection than those under the PDP Law (thereby permitting offshore data transfers from Indonesia to those countries without obtaining consent from data subjects or otherwise requiring the recipient of the data to implement adequate and binding personal data protection measures). The Draft Regulation also clarifies that controllers may only rely on consent as a basis for cross-border transfers in limited circumstances, including that the transfer is not recurring, involves a limited number of data subjects and the controller has informed the PDP Agency and data subject about the transfer and the legitimate interests of making it.
- ***Data Protection Impact Assessments (DPIAs)*** – the Draft Regulation provides detailed guidance on the processing of high-risk personal data, including on the requirements for undertaking a DPIA. In particular, the Draft Regulation obligates controllers, as part of a DPIA, to systematically describe their personal data processing activities, assess the necessity and proportionality of the processing, conduct a risk assessment to safeguard the rights of data subjects and document the measures taken to protect data subjects from identified risks.

E. Hong Kong

Hong Kong's Personal Data (Privacy) Ordinance ("**PDPO**") has not undergone any substantive amendment since changes were introduced in 2021 to combat doxxing acts which intrude on personal data privacy. Despite this, it is expected that the Hong Kong Government will – in coming years – seek to update the PDPO to bring it in line with more robust international privacy regimes such as the PIPL and GDPR. On 29 June 2023, China's CAC and Hong Kong's Innovation, Technology and Industry Bureau ("**ITIB**") signed a memorandum of understanding ("**MoU**") for data transfers within the Great Bay Area ("**GBA**", covering cities in the Guangdong province and Hong Kong). The contents of the MoU were not made public, however, in a press release, the ITIB indicated that it is intended to facilitate data flows between the PRC and Hong Kong and to provide a convenient channel for this purpose.[72] Subsequent to agreement of the MoU – and as noted in the summary for China above – the National Information Security Standardization Technical Committee ("**TC260**") published the Draft GBA Guidelines, proposing a draft certification regime for cross-border data transfers within the GBA.[73] The Draft GBA Guidelines ease certain PIPL requirements for cross-border data transfers, however go beyond those under the PDPO by requiring data exporters to enter into a legally binding agreement, comply with additional security and notification requirements and take substantive steps to prevent the onward transfer of data to third countries. In light of this, utilisation of the certification regime in its current form is likely to be limited to PRC-based

data exporters with affiliates in Hong Kong – whereas Hong Kong-based data exporters with affiliates in the PRC will presumably eschew certification in favour of the less restrictive PDPO regime. In any event, the precise application of the regime proposed under the Draft GBA Guidelines remains to be seen, with details regarding the certification procedure and enforcement of the Draft GBA Guidelines yet to be published. On the enforcement front, the Hong Kong Office of the Privacy Commissioner for Personal Data ("**PCPD**") published its report on 1 June 2023 concerning the investigation of Softmedia Technology Company Limited for alleged failures to take adequate security measures to protect personal data stored in a credit reference platform. The PCPD found that Softmedia had breached Data Protection Principles 4 (Security) and 2(2) (Retention) by allowing access to credit data to at least eight lenders without obtaining evidence of the complainant data subject's authorisation to do so and by retaining more than 50,000 credit records of borrowers who had completed their repayments over five years prior.[74] The PCPD's findings clarify that:

- "personal data" includes pseudonymised data for the purposes the PDPO;
- Data Protection Principle 4 (Security) requires organisations to take active steps to secure personal data against unauthorised access where necessary (e.g., by restricting the frequency of access, requiring strong login passwords and/or imposing periodic password changes); and
- Data Protection Principle 2(2) (Retention) places the onus on the controller and not data subjects to assess an appropriate data retention period (i.e., it was insufficient that Softmedia permitted data subjects to request removal of their credit from the platform from five years following repayment).

In response to the breaches, the PCPD issued an enforcement notice requiring Softmedia to take remedial and preventative actions, including deleting credit data in respect of which more than five years had elapsed and formulating policies and measures to restrict access to the credit reference platform.

F. Japan

2023 saw limited domestic activity with regard to data protection in Japan. In March, Japan's Ministry of Internal Affairs and Communications sought public opinions on the revised draft of the Telecommunications Business Act. The draft changes to the law add guidelines to ensure the protection of personal information by telecommunications companies. Public consultation closed on 24 April 2023.[75] Despite this, various joint initiatives between Japan and foreign governments and data protection authorities were announced in the second half of the year:

- On 17 October 2023, Japan's Personal Information Protection Commission and the UK's Information Commissioner's Office announced the signing of a Memorandum of Understanding ("**MoU**") focused on data protection.[76] The MoU provides that the respective authorities will share certain information regarding investigations. The authorities will not share personal information under the MoU (other than in exceptional cases).
- On 28 October 2023, Japan and the EU concluded a deal on cross-border data flows at the EU-Japan High Level Economic Dialogue.[77] Once ratified, the agreed provisions will be included in the EU-Japan Economic Partnership Agreement. The deal will allow both parties to "handle data efficiently without cumbersome administrative or storage requirements, and provide them with a predictable legal environment". An important element of the deal is the removal of requirements for companies to physically store their data locally.
- On 14 November 2023, the Japan-U.S. Economic Policy Consultative Committee released a joint statement indicating their joint desire to continue collaborating to facilitate cross-border data flows and effective data and privacy protections globally.[78] In support of their efforts to do so, the two nations plan to coordinate

bilaterally and multilaterally on outreach to partners to promote expansion of the Global Cross-Border Privacy Rules (CBPR) Forum.

G. New Zealand

Following the recommendations of New Zealand's Ministry of Justice in its 2022 consultation paper (summarised in the 2023 International Outlook and Review), the Government introduced a Privacy Amendment Bill into New Zealand Parliament in October 2023, proposing new notification requirements related to the indirect collection of personal data.[79] If the Bill is passed, organisations will need to take reasonable steps to ensure that data subjects are aware of certain details regarding the indirect collection of their personal data, including that their personal data has been collected, why it has been collected, who it will be shared with and what their rights are. Organisations must take these steps as soon as is reasonably practicable after the indirect collection of the relevant personal data, unless the individual has already been made aware of the required matters (e.g., by the entity which performed the direct collection). The Bill also provides for exemptions in certain circumstances – for example, where non-compliance would not prejudice the interests of the individual, compliance would prejudice the purposes of the collection or compliance would not be reasonably practicable in the circumstances. If passed, the changes in the Bill will be subject to a grace period and will not apply to personal data collected before 1 June 2025. The Bill nonetheless remains subject to public comment, as well as the various steps of the New Zealand legislative process.

H. Philippines

On 7 November 2023, the National Privacy Commission ("**NPC**") issued Advisory No. 2023-01 (the "**Advisory**"), which provides further clarity on how personal information controllers ("**PICs**") and personal information processors ("**PIPs**") should avoid practices involving deceptive design patterns, which refer to "design techniques embedded on an analog or digital interface that aim to manipulate or deceive a data subject to perform a specific act", in connection with the processing of personal data.[80] The Advisory reminds PICs and PIPs to abide by the principle of fairness, and to ensure that personal data is processed in a manner that is "neither manipulative nor unduly oppressive to a data subject". The Advisory covers best practices concerning both Appearance-Based and Content-Based Deceptive Designs, and provides a non-exhaustive list of prevalent deceptive design patterns to avoid, including, among others, purposely complicating or muddling a data subject's choices relating to the processing of personal data and the use of ambiguous language to nudge data subjects into making a choice that is detrimental or violative of their rights as a data subject.

I. Singapore

On 18 July 2023, Singapore's Personal Data Protection Commission ("**PDPC**") published draft Advisory Guidelines on the use of Personal Data in AI Recommendation and Decision Systems.[81] The Guidelines aim to clarify how the Personal Data Protection Act 2012 ("**PDPA**") applies to the collection and use of personal data by organisations in order to develop and deploy systems that embed machine learning ("**ML**") models which are then used to make decisions autonomously or to assist a human decision-maker through recommendations and predictions ("**AI Systems**"). The Guidelines are advisory in nature and are not legally binding, however provide a useful indication as to how the PDPC intends to interpret the PDPA in light of the increasingly important intersection between AI and data privacy. The Guidelines clarify that where organisations intend to use personal data to develop, test or monitor AI Systems, they may be able to rely on either the business improvement and/or research exemptions under the PDPA in place of obtaining data subjects' consent. The Guidelines set out relevant considerations for organisations intending to rely on either exception, but clarify that in doing so, organisations must nonetheless adopt appropriate technical, process and/or legal controls for data protection as required by the PDPA. The Guidelines also recommend that organisations deploying AI Systems should ensure that they provide individuals with information on how their

personal data is used in deployed AI Systems. In addition to the release of the Guidelines, enforcement decisions published by the PDPC in 2023 generated important takeaways in the context of the PDPA, including that:

- organisations should implement multi-factor authentication for admin accounts with access to confidential or sensitive personal data or large volumes of personal;[82] and
- broad catch all obligations to comply with data protection standards may not be a sufficient administrative protection in the context of engaging third-party vendors and organisations may need to include specific obligations as relevant to the individual engagement.[83]

Consistent with the global trend in uplifting online content and child safety regulations, Singapore's Info-communications Media Development Authority ("**IMDA**") released the final version of the Code of Practice for Online Safety on 17 July 2023.[84] The Code applies since 18 July 2023 to designated social media services. The Code imposes specific obligations on these social media services with respect to user safety, user reporting/resolution and accountability. The maximum penalty for non-compliance with the Code is SGD 1 million, however, it remains to be seen how the IMDA will enforce its provisions in practice other than via the online safety reports that covered providers are required to submit on an annual basis. On 12 December 2023, the Cyber Security Agency of Singapore ("**CSA**") announced a public consultation that ended on 15 January 2024 to seek views on its draft amendments to the Cybersecurity Act 2018, which is the legislative framework that governs the oversight and maintenance of national cybersecurity in Singapore.[85] Notably, these amendments extend the Commissioner of Cybersecurity's oversight to include Foundational Digital Infrastructure (FDI) such as data centres, cloud computing providers and internet exchanges, and enhance its powers to authorise an onsite inspection to ascertain compliance. In addition, the CSA has sought to expand the scope of reportable incidents for providers to include incidents involving other computers or computer systems which are controlled by owners or providers of essential services, irrespective of whether such systems are interconnected to, or communicate with, critical information infrastructures.

J. South Korea

Amendments and enforcement decrees to the Personal Information Protection Act ("**PIPA**") came into force on 15 September 2023.[86] The amendments are considered a major overhaul in Korea's data protection law, and will notably "streamline inconsistencies in data processing standards disparately applied to online and offline businesses" to help prepare the industry for a "full-fledged digital transformation". Key amendments include the following:

- ***Rights of Data Subjects*** – The Personal Information Protection Commission ("**PIPC**") will implement more flexible data processing procedures where there is an urgent need to collect, use or provide personal data in order to protect data subjects from physical threats or to mitigate public health crises. Furthermore, privacy-related dispute resolution procedures have been revised to streamline the process of providing appropriate remedies to data subjects whose rights may have been infringed. Most notably, both public institutions and private companies are now mandated to participate in dispute resolution proceedings.
- ***Regulations Governing Online and Offline Entities*** – The inconsistent standards which have been applied to online and offline businesses have been streamlined and are now subject to the same set of regulations, including (1) a reporting and notification timeline for data breaches, (2) a requirement to obtain consent from legal guardians for collection and use of personal data of children under 14 and (3) application of consistent criteria for imposing administrative sanctions.

- ***Public Institutions Handling Large Data Sets*** – Data safety measures have been strengthened for operators of major public systems that handle large amounts of personal data of Korean citizens. Under the new measures, covered entities are required to: (1) conduct more robust analysis and inspection of access records, (2) designate a manager responsible for each system and (3) make notifications regarding incidents involving unauthorised access to personal data using public systems.
- ***Cross-Border Data Transfers*** – The amendment addresses the conditions for cross-border data transfers and the penalties for the associated transgressions. The transfer of personal data to other countries is permitted if (1) the destination country provides the same level of data protection as Korea or (2) the transfer is made to "certain certified companies". Concerning the associated penalties, the amendment changes the basis for calculating the maximum penalty from "total revenue related to the violation" to "total revenue minus the amount of revenue incurred from activities not related to the violation". This amendment was introduced to prevent penalties from becoming excessive and beyond the scope of the associated transgression.

K. Sri Lanka

The Sri Lankan Government continued to take steps to implement the Personal Data Protection Act No. 9 of 2022 – announcing plans in September 2023 to establish a Data Protection Authority and to finalise additional cybersecurity legislation.[87] The Sri Lankan Government also commenced a unique identity card project in 2023, involving the collection of biographic and biometric information from citizens, including facial, iris and fingerprint data. According to Sri Lankan Government officials, the project is expected to store the personal data of all individuals in a centralised system for the purpose of issuing identification cards. India has provided aid of 450 million Indian rupees to fund the project.

L. Thailand

On 25 December 2023, Thailand's Personal Data Protection Committee (the "**PDPC**") published two notifications, the Adequacy Country Notification and the Appropriate Safeguard Notification, which regulate cross-border transfers of personal data under Sections 28 and 29 of the Thailand's Personal Data Protection Act (the "**PDPA**").[88] The notifications are expected to take effect on 24 March 2024.

- The Adequacy Country Notification establishes the rules for determining whether a destination country or other international organisation meets the minimum requirements for cross-border transfers. The assessment involves (1) assessment of the destination country's legal safeguards against the PDPA, including in areas such as security, data subject rights and legal remedies, and (2) confirmation that a competent and independent regulatory body has been established in the destination country that is capable of enforcing relevant data protection laws. The PDPC also has the power to establish a whitelist of approved destination countries and retains the power to determine the adequacy of a destination country as a data transfer recipient.
- The Appropriate Safeguard Notification serves as an exception to the Adequacy Country Notification, and allows for data transfers through Binding Corporate Rules ("**BCRs**") in instances where the transferee is affiliated with the transferor. A covered entity must obtain the approval of PDPC to the terms of BCRs prior to adopting them. In instances where: (1) a destination country or other international organisation does not meet the minimum requirements for receiving personal data transfers; and (2) BCRs cannot be adopted, the Appropriate Safeguard Notification mandates the implementation of other safeguards before initiating any cross-border personal data transfers, such as by entering into standard contractual clauses.

On the enforcement front, multiple decisions by the Expert Committee (formed under the PDPA) in October and November 2023 indicate that the authority is likely to take a more proactive approach to enforcement going forward. The de facto grace period that followed the PDPA taking effect on 1 June 2022 now appears to be over and the Expert Committee may consider utilising its enforcement powers to impose administrative fines and penalties for non-compliance.

M. Vietnam

As explained in the 2023 International Outlook and Review, the Vietnamese data protection framework has historically been fragmented across various different laws. In order to consolidate the obligations of covered entities into a single omnibus law, the Vietnamese Government issued the Decree on Personal Data Protection ("**PDPD**") as Decree No. 13/2023/ND-CP on 17 April 2023.[89] Notably, the PDPD will not replace but continue to exist concurrently with other existing laws. Key features of the PDPD include the following.

- ***Scope of the Law*** – The PDPD applies to Vietnamese individuals and organisations (including those operating offshore) and also to foreign entities operating in Vietnam, or directly engaging in or relating to personal data processing activities in Vietnam.
- ***Classification of Personal Data*** – The PDPD classifies personal data into two groups of "basic personal data" and "sensitive personal data". The list of sensitive personal data is broad and non-exhaustive, including any personal data associated with an individual's privacy that, when infringed, directly affects their rights and interests.
- ***Classification of Processing Entities*** – As implied under the draft Cybersecurity Administrative Sanctions Decree, the PDPD recognises the concepts of "personal data controller" and "personal data processor" which are broadly consistent with the equivalent terms under the GDPR. It also introduces the concept of "personal data controlling and processing entity" (which has the functions of both a controller and the processor).
- ***Processing Principles*** – The PDPD introduces eight principles for the processing of personal data: lawfulness, transparency, purpose limitation, data minimisation, accuracy, integrity, confidentiality and security, storage limitation and accountability. While these principles are also enshrined in the GDPR, the PDPD departs from the EU model insofar as it does not recognise the principle of "legitimate interests".
- ***Consent*** – The PDPD adopts a consent-centric approach, requiring controllers to obtain consent to data subjects and to notify the data subject about the purpose, nature and scope of processing. A data subject must express their consent clearly and specifically in writing, by voice, by ticking a consent box, by text message, by selecting consent technical settings, or via another action which demonstrates the same. Processing of personal data without consent is nonetheless permissible in certain limited circumstances (e.g., where necessary to protect the life or health of the data subject, in accordance with law or to fulfil the contractual obligations of the data subject).
- ***Cross-Border Data Transfers*** – The PDPD imposes new requirements for cross-border data transfers, including that the transferor must create a Dossier of Impact Assessment for the Cross-Border Transfer of Personal Data ("**TIA Dossier**") before transferring personal data out of Vietnam. The TIA Dossier must contain the information prescribed by the PDPD and be made available at all times for the inspection and evaluation by the authority. In addition, the transferor must submit one original copy of the TIA Dossier to the Department of Cybersecurity and Hi-Tech Crime Prevention ("**A05**"), an authority under the Ministry of Public Security of Vietnam ("**MPS**") within 60 days from the date of the personal data processing.

Notably, the MPS has the power to halt cross-border data transfers if (i) the data is used for activities that violate the interests and national security of Vietnam; (ii) the transferor fails to complete or update the TIA Dossier; or (iii) the personal data of Vietnamese citizens is disclosed or lost.

- ***Rights of Data Subjects*** – Eleven rights of the data subject are enshrined in the PDPD, including (i) the right to be informed, (ii) the right to consent, (iii) the right to access, (iv) the right to withdraw consent, (v) the right to delete data, (vi) the right to restrict data processing, (vii) the right to data provision, (viii) the right to object to data processing, (ix) the right to complain and denounce and/or initiate lawsuits, (x) the right to claim compensation for damages and (xi) the right to self-defence. Responses to requests for the exercise of the rights set out in (iii), (v), (vi), (vii) and (viii) are subject to a 72-hour deadline.

The PDPD took effect on 1 July 2023 without any grace period (other than a two-year grace period for the appointment of a data protection officer or department by small- and medium-sized enterprises). While it is uncertain whether the authorities will enforce the PDP's requirements during the unavoidable transitional period following its implementation, covered entities should nonetheless begin preparing plans for compliance. In this regard, the Vietnamese Government established the National Portal on Personal Data Protection, allowing entities to take streamlined measures for compliance with the new law, including online submission of data protection impact assessments and data breach notifications.[90]

V. Developments in Africa

A. Kenya

Following a petition to introduce a Bill on Robotics and AI on 29 November 2023, politicians and stakeholders are currently debating AI regulation in Kenya. The Bill foresees the creation of a professional regulating body overseeing the activities of AI practitioners and imposing license fees for those working in the sector, whilst guaranteeing government funding for AI research and development.[91]

B. Nigeria

On 14 June 2023, the Nigerian Data Protection Bill 2023 (available here) entered into force. It sets out general principles for the processing of personal information, including the processing of sensitive information, controller obligations, such as breach notifications, Data Protection Impact Assessments and the appointment of a data protection officer ("**DPO**"). Furthermore, the Bill imposes restrictions on cross-border transfer of personal information and establishes data subject rights, namely, the right to object, withdraw consent, data portability and the right not to be subject to a decision based solely on the automated processing of personal data. On 15 December 2023, the National Data Protection Bureau ("**NDPB**") issued a code of conduct for data protection compliance organisations ("**DPCO**"). In particular, the code outlines registration requirements for DPCOs, personal and professional requirements of their DPOs.[92]

C. Tanzania

On 1 May 2023, the Personal Data Protection Act 2022 entered into force.[93] Complementing that, the Ministry of Information, Communication and Information Technology published Regulations on the collection and processing of personal data and a complaints handling procedure.[94]

D. Other African Jurisdictions

After its adoption by the African Union ("**AU**") in 2014, the African Union Convention on Cyber Security and Personal Data Protection (also known as "**Malabo Convention**") came into effect on 8 June 2023, after Mauritania was the 15th country to ratify it on 9 May 2023. To date, 15 of the AU's 55 countries have signed and ratified the treaty, and 12

more have already signed it.[95] In Algeria, the Law Relating to the Protection of Individuals in the Processing of Personal Data came into force on 11 August 2023, applying to the processing of personal data by public bodies or private individuals.[96] In Malawi, the Parliament introduced Bill No. 22 for the Data Protection Act, 2023 on 7 December 2023, aiming to provide a comprehensive legal framework for the regulation of personal data.[97] **VI. Other Developments in the Middle East**

A. Israel

Following last year's review, Israeli privacy protection regulations on data transfers from the European Economic Area were published in their final form on 7 May 2023.[98] Furthermore, a corresponding Q&A has been issued.[99] The Privacy Protection Authority ("**PPA**") published a guidance paper on Internet of Things ("**IoT**") products and smart homes. It requires companies to secure their databases in accordance with the requirements of the Protection of Privacy Regulations (Data Security) 5777-2017 ("**Data Security Regulations**").[100] Jointly, the Ministry of Innovation, Science, and Technology, the Office of Legal Counsel and Legislative Affairs at the Ministry of Justice published Israel's recent policy on Artificial Intelligence Regulations and Ethics 2023, aiming to foster responsible innovation in the private sector.[101]

B. Saudi Arabia

The Council of Ministers approved amendments to the data protection law, previously introduced by the Saudi Data and Artificial Intelligence Authority ("**SDAIA**"). These include the right to data portability, legitimate interests as a legal basis for processing in some particular circumstances, permitting the processing of personal data for marketing purposes where a clear mechanism is provided to allow the target recipients to request the cessation of the processing, permitting data transfers outside Saudi in specific circumstances and in accordance with certain conditions; and a requirement to keep records of the operations performed on personal data and set rules to restrict access to such data.[102] On 14 September 2023, the Personal Data Protection Law ("**PDPL**"), the Regulations on Personal Data Transfers and several implementing regulations entered into force. Compliance will be mandatory one year later.[103] On the same day, the SDAIA published their Artificial Intelligence Ethics Framework 2.0, focusing on helping companies develop responsible AI-based solutions and limiting negative implications of AI systems, while encouraging innovation.[104] On 27 November 2023, the SDAIA announced the launch of various initiatives, including the National Data Governance Platform, serving to register entities falling under the scope of the PDPL.[105] On 20 December 2023, the SDAIA announced the publication of a guide on generative AI in an effort to raise the level of awareness about the importance of AI technologies.[106]

C. Other Middle East Jurisdictions

In several countries, various laws on digital regulation and data protection have been published, entered into force or are under review:

- On 15 November 2023, the Abu Dhabi Global Market ("**ADGM**") Office of Data Protection ("**ODP**") issued and adopted an Addendum to the European Commission's Standard Contractual Clauses ("**EU SCCs**") for personal data transfers.[107] Companies who had already implemented the EU SCCs shall be able to use the Addendum as a data transfer mechanism to comply with the ADGM Data Protection Regulations 2021. In addition, the ODP also issued guidelines to support businesses in implementing the Addendum to their existing EU SCCs.[108]
- Dubai International Financial Centre's ("**DIFC**") Regulation 10 on Processing Personal Data Through Autonomous and Semi-Autonomous Systems (amending the Data Protection Regulations 2020) entered into force on the date of its publication on 1 September 2023.[109] Additional guidance has been updated accordingly.[110]

- Jordan finalised and published its Personal Data Protection Law in its Official Gazette on 17 September 2023. The law will enter into force six months after its publication.[111]
- In Oman, the Data protection law entered into force on 13 February 2023, one year after its publication in the Official Gazette.[112]
- The Qatar Financial Centre ("**QFC**") issued a third version of the QFC Data Protection Rules on 10 December 2023.[113] Although broadly similar to the previous rules, the introduction of new requirements for the use of Corporate Rules for transfers of personal data outside the QFC constitutes a key change.

VII. Developments in Latin America and in the Caribbean Area

A. Argentina

On 5 April 2023, the Argentinian data protection authority ("**AAIP**") published its 2022 management report, including a new Personal Data Protection Bill, largely in line with the draft bill released in November 2022. On 30 June 2023, the draft has been passed to Congress, where it may be subject to further changes.[114] Upon passing, according to the current draft, its provisions will enter into force 180 days after its publication in the Official Gazette, except for the section on administrative sanctions, which will enter into force once it has been published. On 17 April 2023, the AAIP deposited the instruments of ratification of the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (also known as "**Convention 108+**"), strengthening individual data protection.[115] On 26 September 2023, it was announced that the Uruguayan data protection authority had signed a cooperation agreement with the AAIP, including an exchange of investigation results. Furthermore, the agreement is aimed at coordinating strategies and activities to strengthen data protection in Uruguay and Argentina. Additionally, the agreement shall facilitate collaboration in various areas such as the preparation of recommendations, guides and other documents.[116] On 18 October 2023, the AAIP published approved Standard Contractual Clauses ("**SCCs**") for international data transfers, as proposed by the Ibero-American Network for the Protection of Personal Data ("**RIPD**"). These clauses are part of a guide for the implementation of model contractual clauses for the international transfer of personal data, facilitating the transfer of personal data from countries that are members of the RIPD to other jurisdictions.[117]

B. Brazil 1. AI Act (Brazil)

In December 2022, the Brazilian Senate's Commission of Jurists approved a draft for the Brazilian AI Act, which was converted into Bill No. 2338/2023 in the beginning of 2023. The Brazil's draft relies on a risk-based approach and has several points of interaction with the Brazilian General Data Protection Law ("**LGPD**"). Besides, it foresees specific rights to people affected by AI systems, including the right to be informed about interactions with AI systems, the right to contest decisions, the right to human participation and the right to explanation. If approved, the Brazilian AI Act will define sanctions for non-compliance with the law, such as a simple fine of up to BRL 50,000,000 (approx. USD 1 million) per violation – for private legal entities, of up to 2% of the total revenue its group or conglomerate in Brazil obtained in the previous fiscal year (excluding taxes) – as well as the temporary or permanent suspension (partial or total) of the development, supply or operation of AI systems, and a prohibition on processing related databases.[118] For any regulatory and enforcement matters the National Data Protection Authority ("**ANPD**") has already positioned itself offering to act as the key authority. On 3 October 2023, the ANPD also published a call for contributions on its regulatory sandbox pilot program, consisting of a controlled environment to test technologies associated with AI developed by participants. Currently, the draft is being processed in the Federal Senate in an internal committee to resolve open questions.[119] Besides national efforts to regulate AI, the states Ceará in 2021 and Alagoas in November 2023 already passed first laws regulating AI.[120]

2. Other Developments in Brazil

On 27 February 2023, the ANPD published its finalised resolution on the application of the administrative sanctioning system for violations of personal data law. It comprises a multi-layered system including warnings, simple fines, daily fines, the blocking and/or deletion of personal data relating to the offence, as well as partial or total bans on activities related to data processing. It also provides a tiered classification system and outlines various criteria and parameters that will be considered when imposing sanctions.[121] Throughout the year, the ANPD issued various clarifications on debated topics, including inter alia:

- The clarification that the LGPD only applies to the processing of personal data of living natural persons and that data relating to a deceased person does not constitute personal data and is therefore not subject to the LGPD's protection; and[122]
- Open questions on DPO compliance and performance under LGPD. The requirements associated with conducting Data Protection Impact Assessments ("**DPIA**") were addressed too.[123]

C. Chile

Chile's regulation on the protection of privacy and personal data is currently under a lengthy reformation process, drawing inspiration from the EU GDPR. In 2023, the proposed new bill has been passed to the Senate, where it is now subject to further discussion. To date, the proposal has been referred to a Joint Committee at the beginning of January 2024 to resolve disagreement between the two Chambers over articles.[124]

D. Colombia

On 6 July 2023, the Colombian data protection authority ("**SIC**") announced its decision to fine a company COP 1,306,289,600 (approx. USD 336,000), which is the highest fine relating to the violation of data protection laws to date.[125] The SIC furthermore issued a corrective order for violation of general provisions protecting personal data. The fine was based on a failure to implement adequate and sufficient measures to obtain referral telephone numbers from its customers via a marketing campaign with prior, express and informed consent of the data subjects. On 4 August 2023, the SIC also published its Official Guide to Personal Data Protection.[126] On 31 August 2023, the Chamber of Representatives of Colombia initiated the legislative process to adopt a general regime for the protection of personal data ("**Bill 156/2023C**"). It shall further cover the protection of fundamental rights, including the fundamental right of personal data protection, under the terms described in Article 15 and Article 20 of the Colombian Constitution.[127]

E. Mexico

On 7 February 2023, the National Institute for Access to Information and Protection of Personal Data ("**INAI**") published its interpretation criteria for personal data law.[128] In the course of the publication of its 2024 budget, the INAI also published plans to review and amend the Federal Law on Protection of Personal Data Held by Private Parties in light of the recent developments in generative AI.[129]

F. Paraguay

On 29 August 2023, the Chamber of Deputies of Paraguay announced that the Commission of Industry, Commerce, Tourism, and Cooperativism issued a favourable opinion on the bill on the Protection of Personal Data of the Republic of Paraguay, which was presented first in 2021.[130]

G. Peru

The Ministry of Justice and Human Rights is currently conducting a review of the regulations of the law on transparency and access to public information, aiming to optimise the current regulation and integrate improvements to the procedure for access to information, as a comprehensive review of current regulations is deemed necessary.[131] Furthermore, it announced a draft for Law No. 29733 on Personal Data Protection. In particular, the draft aims to raise the regulatory standards for the protection of personal data compared to the previous regulations.[132]

H. Uruguay

On 21 November 2023, the Uruguayan data protection authority ("**URCDP**") published a favourable Adequacy Resolution No. 63/2023 on data protection for cross-border data transfers with South Korea and entities under the EU-U.S. Data Privacy Framework [133] . The adequacy decision from the URCDP followed similar decisions by the European Commission on data transfers between South Korea and the EU-U.S. Data Privacy Framework. **VIII. Developments in Other Latin American and Caribbean Jurisdictions**

A. Bermuda

Following an announcement of the Bermuda Office of the Privacy Commissioner ("**PrivCom**") in June 2023, the Personal Information Protection Act 2016 ("**PIPA**") will be officially implemented on 1 January 2025. Entities operating in Bermuda were therefore given 18 months to prepare for the full implementation of PIPA.[134] To strengthen its resources, PrivCom announced on 24 February 2023, that it had entered into international enforcement cooperation agreements with the Global Privacy Enforcement Network and the Global Privacy Assembly's Enforcement Cooperation Arrangement.[135]

B. Bolivia

The general regulation of data protection is currently subject of a fierce debate in Bolivia, which is currently lacking a comprehensive legal framework on this topic. In this debate, on 31 March 2023, the Agency of Electronic Government and Information and Communication Technologies presented a new data protection bill to the Bolivian Senate, seeking to introduce, inter alia, a new data protection agency.[136] Separately, a motion for the reintroduction in the Legislative Assembly of bill No. 349/2020-2021 for the protection of personal data was filed, on 3 March 2023.[137]

C. Costa Rica

On 10 November 2023, the Ministry of Science, Technology and Telecommunications has published its national cybersecurity strategy.[138]

D. Grenada

On 10 May 2023, the Grenada Data Protection Act, No. 1 of 2023 has been published in the Official Gazette. It covers, inter alia, the protection of personal data processed by public and private bodies, provides legal bases for processing personal data and sensitive personal data, as well as data protection principles and data subject rights and a penalty system.[139]

E. Guatemala

On 28 April 2023, the President of the Transparency and Probity Commission issued their opinion on Bill No. 6105 of 23 June 2022, for the Approval of the Personal Data Protection Law. Following that, the bill has been returned to Congress and is now subject to further discussions.[140]

F. Guyana

On 16 August 2023, the Data Protection Act No.18 of 2023 has been published in the Official Gazette of Guyana and received Presidential assent.[141]

G. Jamaica

After the Jamaican Data Protection Act entered into force on 1 December 2023, the Information Commissioner granted controllers a six-month grace period for registration under the Data Protection Act.[142] _____ [1] *See* http://curia.europa.eu/juris/document/document.jsf;jsessionid=2BDC80771D0FB7EA8B6F60B9A3C4F572?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=20032710. [2] *See* https://eur-lex.europa.eu/eli/dir/2022/2555. [3] *Id.* [4] *See* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R0868. [5] *See* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554. [6] *See* https://eur-lex.europa.eu/eli/reg/2023/2854. [7] *See* https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042022-calculation-administrative-fines-under_en. [8] *See* https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032021-application-article-651a-gdpr_en. [9] *See* https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052022-use-facial-recognition-technology-area_en. [10] *See* https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82022-identifying-controller-or-processors-lead_en. [11] *See* https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012022-data-subject-rights-right-access_en. [12] *See* https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-92022-personal-data-breach-notification-under_en. [13] *See* https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072022-certification-tool-transfers_en. [14] *See* https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052021-interplay-between-application-article-3_en. [15] *See* https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en. [16] *See* https://edpb.europa.eu/our-work-tools/documents/public-consultations/2023/guidelines-22023-technical-scope-art-53-eprivacy_en [17] *See* https://edpb.europa.eu/our-work-tools/documents/public-consultations/2023/guidelines-012023-article-37-law-enforcement_en [18] *See* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=FR. [19] *See* https://www.cnil.fr/fr/publicite-personnalisee-criteo-sanctionne-dune-amende-de-40-millions-deuros. [20] *See* https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9943230. [21] *See* https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9895080. [22] *See* https://azop.hr/debt-collection-agency-eos-matrix-d-o-o-imposed-with-administrative-fine-in-the-amount-of-5-47-million-euros/. [23] *See* https://edpb.europa.eu/news/national-news/2023/facial-recognition-french-sa-imposes-penalty-payment-clearview-ai_en [24] *See* https://www.imy.se/nyheter/sanktionsavgift-mot-spotify/. [25] *See* https://www.imy.se/nyheter/sanktionsavgift-pa-35-miljoner-mot-trygg-hansa/. [26] *See* https://www.aepd.es/documento/ps-00331-2022.pdf [27] *See* https://edpb.europa.eu/news/national-news/2023/croatian-sa-imposed-administrative-fine-debt-collection-agency-b2-kapital_en. [28] *See* https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2023/varsel-om-gebyr-og-palegg-til-nav/. [29] *See* https://www.imy.se/nyheter/fel-anvanda-kunders-personuppgifter-for-profilering-utan-samtycke/. [30] *See*

https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9910120. [31] *See* https://www.ofcom.org.uk/news-centre/2023/safer-life-online-for-people-in-uk. [32]*See* https://www.ofcom.org.uk/news-centre/2023/tech-firms-must-clamp-down-on-illegal-online-materials?utm_source=tw_graphic&utm_medium=social_org&utm_campaign=onlinesafety23&utm_content=condoc1_press. [33]*See* https://www.ofcom.org.uk/consultations-and-statements/category-1/protecting-people-from-illegal-content-online. [34] *See* https://bills.parliament.uk/bills/3322. [35]*See* https://bills.parliament.uk/bills/3430. [36]*See* https://www.gov.uk/government/news/british-businesses-to-save-billions-under-new-uk-version-of-gdpr. [37]*See* https://ico.org.uk/media/about-the-ico/consultation-responses/4025316/response-to-dpdi-bill-20230530.pdf. [38]*See* https://www.gov.uk/government/publications/uk-us-data-bridge-supporting-documents/uk-us-data-bridge-explainer#:~:text=The%20US%20data%20bridge%20will,required%20to%20maintain%20those%20standards. [39] *See* https://www.dataprivacyframework.gov/. [40] *See* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/. [41]*See* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/ai-and-data-protection-risk-toolkit/. [42]*See* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/toolkit-for-organisations-considering-using-data-analytics/. [43]*See* https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/08/joint-statement-on-data-scraping-and-data-protection/#:~:text=Scraping%20from%20social%20media%20creates,or%20used%20for%20identity%20fraud. [44]*See* https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/direct-marketing-and-regulatory-communications/#who. [45] *See* https://www.fedlex.admin.ch/eli/cc/2022/491/en. [46] *See* https://www.fedlex.admin.ch/eli/oc/2022/568/fr. [47] *See* https://www.edoeb.admin.ch/edoeb/en/home/meldeportale.html. [48] *See* https://www.edoeb.admin.ch/edoeb/de/home/kurzmeldungen/2023/20230404_chatgpt.html. [49] *See* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/ai-and-data-protection-risk-toolkit/. [50] *See* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/toolkit-for-organisations-considering-using-data-analytics/. [51] https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf. [52] https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF. [53] https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf. [54] https://www.homeaffairs.gov.au/help-and-support/how-to-engage-us/consultations/cyber-security-legislative-reforms. [55] http://www.cac.gov.cn/2023-02/24/c_1678884830036813.htm (in Chinese only). [56] http://www.cac.gov.cn/2023-02/24/c_1678884831596384.htm (in Chinese only). [57] http://www.cac.gov.cn/2023-05/30/c_1687090906222927.htm (in Chinese only). [58] http://www.cac.gov.cn/2023-08/03/c_1692628348448092.htm (in Chinese only). [59] http://www.cac.gov.cn/2023-09/28/c_1697558914242877.htm (in Chinese only). [60] https://www.tc260.org.cn/upload/2023-11-01/1698813097992054356.pdf (in Chinese only). [61] https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf. [62] *See* section 3, DPDP Act. [63] *See* section 17(1)(d), DPDP Act. [64] *See* section 9, DPDP Act. [65] *See* sections 4-6, DPDP Act. [66] *See* section 7, DPDP Act. [67] *See* Chapter II, DPDP Act. [68] *See* section 10, DPDP Act. [69] *See* section 16, DPDP Act. [70] *See* section 33 and Schedule, DPDP Act. [71] https://pdp.id/rpp-ppdp/1 (in Bahasa only). [72] https://www.info.gov.hk/gia/general/202306/30/P2023063000219.htm. [73] https://www.tc260.org.cn/upload/2023-11-01/1698813097992054356.pdf (in Chinese only). [74] https://www.pcpd.org.hk/english/enforcement/commissioners_findings/files/r23_21242_e.pdf. [75] https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000188.html (in Japanese only). [76] https://www.ppc.go.jp/files/pdf/ico_moc.pdf. [77]

https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5378. [78] https://www.commerce.gov/news/press-releases/2023/11/joint-statement-japan-us-economic-policy-consultative-committee. [79] https://www.justice.govt.nz/assets/Documents/Publications/Privacy-Amendment-Bill-2023-Approval-for-introduction_FINAL.pdf. [80] https://privacy.gov.ph/wp-content/uploads/2023/11/NPC-Advisory-No.-2023-01-Guidelines-on-Deceptive-Design-Patterns_7Nov23.pdf. [81] https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Legislation-and-Guidelines/Public-Consult-on-Proposed-AG-on-Use-of-PD-in-AI-Recommendation-and-Systems-2023-07-18-Draft-Advisory-Guidelines.pdf. [82] In the matter of an investigation under section 50(1) of the Personal Data Protection Act 2012 and Tokyo Century Leasing (Singapore) Pte. Ltd. [2023] SGPDPC 9 (https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Commissions-Decisions/GD_Tokyo_Century_Leasing_040923.pdf). [83] In the matter of an investigation under section 50(1) of the Personal Data Protection Act 2012 and Ascentis Pte. Ltd. [2023] SGPDPC 10 (see https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Commissions-Decisions/GD_Ascentis_12092023.pdf). [84] https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/imdas-online-safety-code-comes-into-effect. [85] https://www.reach.gov.sg/docs/default-source/participate/public-consultation/cyber-security-agency-of-singapore-(csa)/public-consultations-paper---cybersecurity-amendment-bill.pdf. [86] *See* https://www.pipc.go.kr/eng/user/ltn/new/noticeDetail.do?bbsId=BBSMSTR_000000000001&nttId=2331. [87] https://economynext.com/sri-lanka-says-measures-taken-to-ensure-digital-security-of-indian-funded-unique-id-project-130540/. [88] *See* https://www.dataprotectionreport.com/2024/01/thailand-the-regulation-with-respect-to-cross-border-transfer-of-personal-data/. [89] https://www.dataguidance.com/news/vietnam-decree-protection-personal-data-enters-force; https://thuvienphapluat.vn/van-ban/EN/Cong-nghe-thong-tin/Decree-No-13-2023-ND-CP-dated-April-17-2023-on-protection-of-personal-data/564343/tieng-anh.aspx. [90] https://rouse.com/insights/news/2023/vietnam-government-launches-national-portal-on-personal-data-protection#:~:text=Vietnam%3A%20Government%20Launches%20National%20Portal%20on%20Personal%20Data%20Protection,-Published%20on%2018&text=In%20line%20with%20Article%2029.2,vn%2F%20(PDP%20Portal). [91] *See* here (press release) or here (bill proposal). [92] *See* here. [93] *See* here (Swahili). [94] *See* here and here (Swahili). [95] *See* here for full text and status list. [96] *See* here. [97] *See* draft here. [98] *See* here, in Hebrew and English. [99] *See* here (Hebrew). [100] *See* here (Hebrew). [101] *See* here. [102] *See* previous proposals here. [103] *See* here for PDPL; here for the Implementing Regulation; here (Arabic) for the Regulations on Transferring Personal Data. [104] *See* here. [105] *See* here (press release, Arabic). [106] *See* here (Arabic). [107] *See* here. [108] *See* here. [109] *See* here (press release). [110] *See* here, for example the updated DIFC EDMRI Guidance - December 2023. [111] *See* here (Arabic). [112] *See* here (Arabic). [113] *See* here. [114] *See* here. [115] *See* here (press release). [116] *See* here (Spanish). [117] *See* here (Resolution, Spanish). [118] For draft, *see* here (Portuguese). [119] *See* here, for the status of the legislative progress (Portuguese). [120] Lei 607/2023 (Alagoas) available here; Lei Nº 17.611, 11 de Agosto de 2021(Ceará) available here (Portuguese). [121] *See* here (Portuguese). [122] *See* here (Technical Note, Portuguese). [123] *See* here (press release). [124] *See* here (Spanish). [125] *See* here (press release, Spanish). [126] *See* here (Spanish). [127] *See* here, available for download here (Spanish). [128] Available for download here (Spanish). [129] *See* here (Spanish). [130] For legislative status, *see* here (Spanish). [131] *See* here (Spanish). [132] *See* here (Spanish). [133] *See* here (Spanish). [134] *See* here. [135] *See* here. [136] *See* here (press release, Spanish). [137] *See* here (Spanish). [138] *See* here. [139] Available for download here. [140] *See* here. [141] Available for download here. [142] *See* here (press release).

The following Gibson Dunn lawyers assisted in preparing this alert: Ahmed Baladi, Vera Lukic, Joel Harrison, Connell O'Neill, Clémence Pugnet, Thomas Baculard, Hermine

Hubert, Sarah Villani, Anastasia Katsari, Marcus Seete*, Grace Chong, Nick Hay and QX Toh.

Gibson Dunn lawyers are available to assist in addressing any questions you may have about these developments. Please contact the Gibson Dunn lawyer with whom you usually work, the authors, or any leader or member of the firm's Privacy, Cybersecurity & Data Innovation practice group: **Europe**: Ahmed Baladi – Co-Chair, Paris (+33 (0) 1 56 43 13 00, abaladi@gibsondunn.com) Joel Harrison – Co-Chair, London (+44 20 7071 4289, jharrison@gibsondunn.com) Nicholas Banasevic* – Managing Director, Brussels (+32 2 554 72 40, banasevic@gibsondunn.com) Kai Gesing – Munich (+49 89 189 33-180, kgesing@gibsondunn.com) Vera Lukic – Paris (+33 (0) 1 56 43 13 00, vlukic@gibsondunn.com) Lars Petersen – Frankfurt/Riyadh (+49 69 247 411 525, lpetersen@gibsondunn.com) Robert Spano – London/Paris (+44 20 7071 4000, rspano@gibsondunn.com) **Asia**: Connell O'Neill – Hong Kong (+852 2214 3812, coneill@gibsondunn.com) Jai S. Pathak – Singapore (+65 6507 3683, jpathak@gibsondunn.com) **United States**: S. Ashlie Beringer – Co-Chair, Palo Alto (+1 650.849.5327, aberinger@gibsondunn.com) Jane C. Horvath – Co-Chair, Washington, D.C. (+1 202.955.8505, jhorvath@gibsondunn.com) Rosemarie T. Ring – Co-Chair, San Francisco (+1 415.393.8247, rring@gibsondunn.com) Ryan T. Bergsieker – Denver (+1 303.298.5774, rbergsieker@gibsondunn.com) Gustav W. Eyler – Washington, D.C. (+1 202.955.8610, geyler@gibsondunn.com) Cassandra L. Gaedt-Sheckter – Palo Alto (+1 650.849.5203, cgaedt-sheckter@gibsondunn.com) Svetlana S. Gans – Washington, D.C. (+1 202.955.8657, sgans@gibsondunn.com) Lauren R. Goldman – New York (+1 212.351.2375, lgoldman@gibsondunn.com) Stephenie Gosnell Handler – Washington, D.C. (+1 202.955.8510, shandler@gibsondunn.com) Natalie J. Hausknecht – Denver (+1 303.298.5783, nhausknecht@gibsondunn.com) Martie Kutscher Clark – Palo Alto (+1 650.849.5348, mkutscherclark@gibsondunn.com) Kristin A. Linsley – San Francisco (+1 415.393.8395, klinsley@gibsondunn.com) Timothy W. Loose – Los Angeles (+1 213.229.7746, tloose@gibsondunn.com) Vivek Mohan – Palo Alto (+1 650.849.5345, vmohan@gibsondunn.com) Ashley Rogers – Dallas (+1 214.698.3316, arogers@gibsondunn.com) Alexander H. Southwell – New York (+1 212.351.3981, asouthwell@gibsondunn.com) Eric D. Vandevelde – Los Angeles (+1 213.229.7186, evandevelde@gibsondunn.com) Benjamin B. Wagner – Palo Alto (+1 650.849.5395, bwagner@gibsondunn.com) Debra Wong Yang – Los Angeles (+1 213.229.7472, dwongyang@gibsondunn.com) **Nicholas Banasevic, Managing Director in the firm's Brussels office and an economist by background, is not admitted to practice law. *Marcus Seete, a legal trainee in the Brussels office, is not admitted to practice law.*

Related Capabilities

Privacy, Cybersecurity, and Data Innovation