GIBSON DUNN

International Cybersecurity and Data Privacy Outlook and Review – 2023

Client Alert | February 16, 2023

For the fifth consecutive year, and following the publication of Gibson Dunn's tenth annual U.S. Cybersecurity and Data Privacy Outlook and Review on Data Privacy Day in 2023, we offer this separate International Outlook and Review.

The European Union ("**EU**") supervisory authorities continued to apply and enforce the General Data Protection Regulation ("**GDPR**") vigorously, imposing record-setting fines up to €405 million[1] and with a total amount of approximately €2.92 billion in fines. We can expect that trend to continue in 2023.

There was also a significant number of developments in the evolution of the regulatory landscape for digital services, data sharing and cybersecurity in the EU:

- The European Parliament adopted a set of comprehensive standards to regulate the digital space through the Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market For Digital Services ("Digital Services Act" or "**DSA**")[2] and Regulation (EU) 2022/1925 of 14 September 2022 on contestable and fair markets in the digital sector ("Digital Markets Act" or "**DMA**").[3]
- Furthermore, the Regulation (EU) 2022/868 of 30 May 2022 on European data governance ("**Data Governance Act**")[4] and the Proposal for a Regulation of 23 February 2022 on harmonised rules on fair access to and use of data ("**Data Act**")[5] are part of the European strategy for data, which aims to develop a single market for data by supporting responsible access, sharing and re-use, while respecting the values of the EU and in particular the protection of personal data.[6]
- In terms of cybersecurity, the adoption of the Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union ("**NIS 2 Directive**")[7] enables to achieve a high common level of cybersecurity across Member States. It is complemented by the Proposal for a Regulation of 15 September 2022 on horizontal cybersecurity requirements for products with digital elements ("**Cyber Resilience Act**"),[8] which strengthens cybersecurity rules to protect consumers and businesses from products with inadequate security features. The European Union Agency for Cybersecurity ("**ENISA**") published a Threat Landscape 2022 which describes top threats (e.g., ransomware, malware, social engineering threats, supply-chain attacks), relevant trends, threat actors and attack techniques, as well as impact and motivation analysis.[9]
- In the aftermath of the *Schrems II* ruling, supervisory authorities challenged several companies for using tools leading to illegal data transfers, such as Google Analytics, and released guidance on international transfers.

International authorities have also been actively involved in terms of guidance published, including on the processing of cookies and calculation of administrative fines. In addition, data protection laws continue to be adopted, such as in Indonesia, Tanzania and Oman. International authorities have also issued significant fines, such as the fine imposed by the Cyberspace Administration of China on a Chinese leading mobile transportation platform

Related People

Ahmed Baladi

Vera Lukic

Joel Harrison

Clémence Pugnet

Thomas Baculard

Jocelyn Shih

Connell O'Neill

of RMB 8.000.000.000 (approx. US$1.2 billion) for violations of the PIPL, Cyber Security Law and Data Security Law.[10]

We cover these topics and many more in this year's International Cybersecurity and Data Privacy Outlook and Review.

I. European Union

A. International Data Transfers

1. EU-U.S. Data Transfers

As we indicated in the 2021 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 EU ("**CJEU**").[11] In order to replace the Privacy Shield and to safeguard cross-border data flows, the European Commission launched the process to adopt an adequacy decision for the EU-U.S. Data Privacy Framework. It will notably provide binding safeguards to limit U.S. intelligence authorities access to data to what is necessary and proportionate to protect national security. A Data Protection Review Court will also be created to investigate and resolve complaints of Europeans on access of data by U.S. intelligence authorities.[12]

The draft adequacy decision, which reflects the assessment by the European Commission of the EU-U.S. Data Privacy Framework and concludes that it provides comparable safeguards to those of the EU, has now been published and transmitted to the European Data Protection Board ("**EDPB**") for its opinion. Then, it will seek approval from a committee composed of representatives of the EU Member States before proceeding to the adoption of the final adequacy decision.[13]

In parallel, it should be noted that the transition period to replace the old standard contractual clauses with the new sets of standard contractual clauses, adopted by the European Commission on 4 June 2021 to take into account the *Schrems II ruling*, expired on December 27, 2022.[14] In addition, the European Commission published a Q&A[15] to provide practical guidance on the use of the new standard contractual clauses to assist stakeholders with their compliance efforts. The content of the document will be updated as new questions arise.[16]

In addition, the UK International Data Transfer Agreement ("**IDTA**") and Addendum came into force on 21 March 2022 and replaced standard contractual clauses for international transfers to take into account the *Schrems II* ruling.[17]

In this respect, the European Data Protection Board ("**EDPB**") updated its guidance on international transfers of personal data, namely:

Guidelines 04/2021 on codes of conduct as tools for transfers,[18] which aim to clarify the role of the different actors involved for the setting of a Code that can be used as a tool for transfers.

Recommendations 1/2022 on the application for approval and on the elements and principles to be found in Controller Binding Corporate Rules,[19] which aim to update the former Article 29 documents (WP 256 rev.01), in particular to include *Schrems II* requirements such as transfer impact assessment and government access requests. The Recommendations are open for public consultation until 10 January 2023.

In light of these developments, several Member State **supervisory authorities issued sanctions, statements, and guidance** in relation to matters concerning international data transfers:[20]

1. Several Supervisory Authorities[21] found that Google Analytics' transfers of

personal data to the U.S. did not comply with the GDPR. In this regard, the French Supervisory Authority published guidance[22] on how to use Google Analytics' in a compliant manner, as well as a Q&A[23] on the same topic. The guidance clarifies that the sole modification of Google Analytics' settings, or the encryption of generated identifiers, is not enough to satisfy the requirements of the *Schrems II* ruling, in particular since it does not prevent transfers to the U.S. nor re-identification of data subjects. The Authority assesses that a solution could be the use of a proxy in order to avoid any direct contact between individuals' terminal and Google servers, provided that certain requirements are met;

2. The Spanish Supervisory Authority[24] fined a U.S.-based company €10 million for transferring data to third parties without legal basis and for failure to comply with data subjects' rights;
3. The Danish Supervisory Authority[25] upheld the ban on a municipality's use of a cloud-based workspace until the municipality brings its processing activities in line with the GDPR and carries out a data protection impact assessment that meets GDPR requirements;
4. The Regional Court of Munich[26] ruled that as Google Fonts could be used without submitting IP-addresses to Google by self-hosting the font-embedding service, the transfer of IP-addresses cannot be based on legitimate interest and users' consent was required. In this regard, the Thuringia Data Protection Authority[27] recommended hosting these fonts locally to avoid any link to U.S. servers.

B. Network Information Security ("NIS 2") Directive

The NIS 2 Directive (EU) 2022/2555 of 14 December 2022[28] will set 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 particular, if an incident has a significant impact on the provision of services covered by the NIS 2 Directive, an authority must be notified without undue delay.

As a reminder, the NIS 2 Directive replaced the Network and Information Security ("**NIS**") to respond to the growth of digitalisation and cyber-attacks. The Member States will have to adopt and publish the measures necessary to comply with the NIS 2 Directive by 17 October 2024.[29]

C. Data Governance Act

The Data Governance Act Regulation (EU) 2022/868 of 30 May 2022 is due to apply from 24 September 2023.[30] The Data Governance Act aims to make more data available by regulating the re-use of publicly held, protected data, by boosting data sharing through the regulation of novel data intermediaries and by encouraging the sharing of data for altruistic purposes. It also creates a European Data Innovation Board tasked with advising the Commission on data governance.[31]

D. Digital Services Act ("DSA")

The DSA Regulation (EU) 2022/2065 of 19 October 2022 sets obligations for digital service providers, such as social media or marketplaces, to tackle the spread of illegal content, online disinformation and other societal risks. These requirements aim to be proportionate to the size and risks platforms pose to society, and their violations can be sanctioned by a fine of up to 6% of the provider's worldwide turnover.[32]

Most provisions of the DSA will apply from 17 February 2024, however some apply from 16 November 2022 and online platforms have until 17 February 2023 to publish the number of average monthly active recipients of their service. The European Commission will then assess whether a platform should be designated a very large online platform or search engine, which will increase its obligations. Following the European Commission's designation, the entity in question will have four months to comply with the obligations under the DSA.[33]

E. Digital Markets Act ("DMA")

The DMA Regulation (EU) 2022/1925 of 14 September 2022 sets obligations for large online platforms acting as "gatekeepers" (platforms whose dominant online position make them hard for consumers to avoid). DMA requirements include allowing third parties to inter-operate with a gatekeeper's own services, a prohibition to rank its own services or products more favorably, and an obligation to collect consent to process users' personal data for targeted advertising. Fines will be up 10% of the gatekeeper's total worldwide turnover, or up to 20% in case of repeated non-compliance.[34]

Most of the provisions of the DMA shall apply from 2 May 2023. After that, within two months and at the latest by 3 July 2023, potential gatekeepers will have to notify their core platform services to the Commission if they meet the thresholds established by the DMA.[35]

F. The Digital Operational Resilience Act ("DORA")

The DORA Regulation (EU) 2022/2554 of 14 December 2022 focuses on preventing and mitigating cyber threats. It will apply 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. DORA was published in the EU's Official Journal, on 27 December 2022, it shall enter into force on the 20th day following that of its publication and will apply from 17 January 2025.[36]

G. Data Act

The Data Act Proposal of 23 February 2022 of the European Commission[37] aims at enabling the sharing of industrial data. The Proposal especially includes provisions to (i) allow users of connected devices to access data generated by them, (ii) prevent abuse of contractual imbalances in data sharing contracts, (iii) enable public sector bodies to access and use data held by the private sector that is necessary for exceptional circumstances, and (iv) facilitate user data portability between providers.[38]

On 4 May 2022, the EDPB and European Data Protection Supervisor ("**EDPS**") issued a Joint Opinion on the Proposal for a Data Act.[39] Both Authorities noted that highly sensitive data could be revealed through sharing mechanisms and that additional safeguards are required to ensure that data sharing does not lower the protection of individuals' right to privacy. The authorities pointed out their concerns regarding the oversight mechanism established by the Proposal which may lead to fragmented and incoherent supervision.

H. Cyber Resilience Act

The Cyber Resilience Act Proposal of 15 September 2022 of the European Commission aims to protect both consumers and businesses from products with inadequate security features and thereby ensure a better level of cybersecurity.[40]

In particular, the Proposal introduces mandatory cybersecurity requirements and obligations for manufacturers, as well as importers and distributors, of products with digital elements (i.e., software or hardware product and its remote data processing solutions, defined as any data processing at a distance for which the software is designed and developed by the manufacturer or under its responsibility and the absence of which would prevent the product from performing one of its functions) within the European Union. 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.[41]

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 the higher). In terms of timeline, it still has to be examined by the European Parliament and the Council and, once adopted, companies will have two years to adapt to the new requirements (one year for reporting obligations of manufacturers of incidents/vulnerabilities—if not modified in the final version of the Regulation).[42]

I. Artificial Intelligence Act

The Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) of 21 April 2021, aims to ensure that artificial intelligence systems placed on the EU market and used in the EU are safe and respect existing law on fundamental rights and EU values.[43]

The Council of the EU published, on 3 November 2022, the final version of the compromise text on the Proposal for the AI Act and adopted, on 6 December 2022, its general approach on the Artificial Intelligence Act.[44]

J. EDPB Guidance

Aside from its guidance on international data transfers, the EDPB issued Guidelines on various topics, including:

1. **Guidelines 01/2022 on the right of access**,[45] which aim to provide guidance on how the right of access has to be implemented in practice;
2. **Guidelines 02/2022 on the application of Article 60 GDPR**,[46] which aim to assist supervisory authorities to interpret and apply their own national procedures in such a way that it conforms to and fits in the cooperation under the one-stop-shop mechanism;
3. **Guidelines 3/2022 on Dark patterns in social media platform interfaces**,[47] which offer practical recommendations to designers and users of social media platforms on how to assess and avoid so-called "dark patterns" in social media interfaces that infringe on GDPR requirements;
4. **Guidelines 04/2022 on the calculation of administrative fines under the GDPR**,[48] which aim to harmonize the methodology supervisory authorities use when calculating the amount of fines;
5. **Guidelines 06/2022 on the practical implementation of amicable settlements**,[49] which address inconsistencies in Member States' approach of amicable settlements sought following cross-border complaints;
6. **Guidelines 07/2022 on certification as a tool for transfers**,[50] which aim to provide further clarification on the practical use of this transfer tool;
7. **Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority**,[51] which aim to clarify the notion of main establishment in the context

of joint controllership and take into account the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR;

8. **Guidelines 9/2022 on personal data breach notification under GDPR**,[52] which aim to clarify the notification requirements concerning the personal data breaches at non-EU establishments.

On 12 July 2022, the EDPB and the EDPS adopted a Joint Opinion 03/2022 on the European Commission's proposal for a regulation on the European Health Data Space.[53] The Opinion aims to draw attention to a number of overarching concerns such as the clarification of the interplay between the proposal and the GDPR or Member State laws.

On 14 July 2022, the EDPB issued a document[54] to enhance cooperation between European supervisory authorities, which contains a set of criteria for identifying cross-border cases of strategic importance in different Member States, as well as the process followed by the EDPB to select these cases. The Commission recalls that cases of strategic importance are primarily one-stop-shop cases which are likely to involve a high risk to the rights and freedoms of individuals in several Member States. In particular, several criteria have been defined by the EDPB (e.g., cases related to the intersection of data protection and other legal fields, where a high risk can be assumed, where a data protection impact assessment is required or where there is a large number of complaints in several Member States). Supervisory authorities can propose any case that meets at least one of the criteria listed below to the other supervisory authorities within the framework of the EDPB, in order to be identified as a case of strategic importance for which cooperation will be prioritised and supported by EDPB. The EDPB already agreed on three (undisclosed) cases to start the project.

II. Enforcement by Supervisory Authorities

In 2022, 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**")[55] and the GDPR continued to be applied and enforced by Member States' supervisory authorities which imposed substantial fines. We have gathered below a list of the highest fines published in 2022:

On 6 January 2022, the French Supervisory Authority published a decision issued on 31 December 2021 to fine an American search engine company €150 million (€90 million for one entity and €60 million for another)[56] for not enabling its users to refuse cookies as easily as to accept them. The authority also issued an injunction for the company to enable users located in France to reject cookies as easily as to accept them under three months, subject to a daily penalty of €100,000 in case of delay. On 28 January 2022, the **French Conseil d'Etat** confirmed the **€100 million** fine imposed by the French Supervisory Authority on two entities of an American search engine company on 7 December 2020.[57] The French Conseil d'Etat also held that the one-stop-shop procedure introduced by the GDPR was inapplicable because cookies practices are regulated by the local data protection legislation (the French "Loi informatique et libertés").

On 15 March 2022, the **Irish Supervisory Authority** adopted a decision, imposing a fine of **€17 million** on a social media company,[58] notably for failing to put in place appropriate technical and organizational measures.

Several supervisory authorities pronounced sanctions against an American facial recognition company, including:

- On 10 February 2022, the **Italian Supervisory Authority** fined the company **€20 million** for unlawful biometric profiling of data subjects.[59] The authority found that the company, which maintains a database of more than 10 billion faces

scrapped from public internet sources (including public social media), did not have a legal basis to do so and failed to comply with a number of GDPR requirements such as transparency and storage limitation.

- On 18 May 2022, the **UK Supervisory Authority** fined the company over **£7.5 million** for failing to provide adequate information to data subjects, failing to meet data protection standards for biometric data, the absence of legal basis and a clear data retention policy. Aside from a fine, the ICO also ordered the company to stop obtaining and processing publicly available personal data of UK residents and to delete all UK residents' data from its systems.[60]
- On 13 July 2022, the **Hellenic Supervisory Authority** fined the company **€20 million** for multiple breaches of the GDPR[61] and notably highlights that the company failed to name a representative since the company is not established in the European Union, to lawfully process personal data, to inform the data subject and to ensure the right of access of data subjects.
- On 17 October 2022, the **French Supervisory Authority** fined the company **€20 million** for several breaches of the GDPR.[62] The authority also ordered the company to stop collecting and processing data of individuals residing in France without a legal basis and to delete the data of these persons that it had already collected, within a period of two months. The Authority added a penalty of €000 euros per day of delay beyond these two months.
- On 15 September 2022, the **Irish Supervisory Authority** fined a social media company **€405 million** for breaches relating to the public disclosure of children's personal data using the social media's business features and a public-by-default setting for personal accounts of children.[63] As the Authority was unable to reach consensus with the concerned supervisory authorities, the EDPB issued a binding decision[64] in accordance with the GDPR dispute resolution process. In addition to the fine, the authority imposed a range of corrective measures, including an order to bring the processing into compliance by taking a range of specified remedial actions.
- On 25 November 2022, the **Irish Supervisory Authority** fined a social media company **€265 million** for breaches relating to the public disclosure of collated dataset of data subjects using its services.[65] The authority began this inquiry following media reports about the discovery of a collated dataset of the social media's personal data that had been made available on the internet. The material issues in this inquiry related to compliance to data protection by design and default obligations. In addition to the fine, the Irish Supervisory Authority issued a reprimand and ordered the company to take specified remedial actions.
- On 19 December 2022 the **French Supervisory Authority** imposed a **€60 million** fine, against a company which operates and develops a search engine, in particular for not allowing its users to refuse cookies as easily as accepting them.[66] The authority considered that the company had breached the French Data Protection Act as cookies were set without prior consent of the user, including cookies with an advertising purpose. Also, while the search engine offered a button to accept cookies immediately, it did not offer an equivalent solution to allow the internet user to refuse them as easily. The authority specified that two clicks were needed to refuse all cookies, while only one was needed to accept them.
- In a decision dated 31 December 2022, the **Irish Supervisory Authority** announced the conclusion of two inquiries related to the data processing operations of a social media company.[67] The authority fined the company a total of **€390 million**. Following the consultation of concerned supervisory authorities and the EDPB, the authority found that the company was not entitled to rely on the newly changed contractual legal basis in connection with the delivery of behavioral advertising as part of its services, and that its processing of users' data to date, in purported reliance on the contractual legal basis, amounted to a contravention of article 6 of the GDPR. The company has also been directed to bring its data

processing operations into compliance within a period of three months.

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

A. UK

1. Data Protection and Digital Information Bill

The UK Government published its Data Protection and Digital Information Bill[68] on 18 July 2022, following the Government's response in June to its consultation on reform of the UK's data protection regime. The Bill would make a number of changes to UK data protection law, including: clarifying the circumstances in which an individual is treated as identifiable; removing the requirement for controllers and processors subject to the extraterritorial scope of UK GDPR to appoint a UK representative; replacing the role of Data Protection Officer with designation of a senior responsible individual; changing the requirements for records of processing activities; and amending the provisions dealing with data protection impact assessments and prior consultation with the UK Supervisory Authority ("**ICO**") on high-risk processing.[69]

The Bill would also make a number of changes to the regulation of cookies and similar technologies, notably by expanding the types of cookies for which consent will no longer be required.[70]

Progress on the Bill was paused in September, with the Government claiming that this was "*to allow Ministers to consider the legislation further*"—the Government has not made clear precisely when, or in what form, the Bill will return to Parliament.[71]

2. International Data Transfers – New Standard Contractual Clauses

On 2 February 2022, the ICO published its new International Data Transfer Agreement ("**IDTA**"), along with an International Data Transfer Addendum to the European Commission's new standard contractual clauses (UK Addendum).[72] The IDTA and UK Addendum provide organisations carrying out processing subject to UK GDPR with two options for making international transfers of personal data to countries that are not subject to UK adequacy regulations.

The IDTA and UK Addendum entered into force on 21 March 2022. Under transitional provisions made by the ICO, organisations can continue to rely on the old (pre-June 2021) standard contractual clauses published by the European Commission for contracts entered into on or before 21 September 2022; these transitional provisions will expire on 21 March 2024.[73]

3. International Data Transfers – ICO Guidance and TRA Tool

On 17 November 2022, the ICO published new guidance on international data transfers under UK GDPR.[74] The new guidance includes a section on carrying out transfer risk assessments ("TRAs"), including a TRA tool.

The ICO's guidance states that an organisation must carry out a TRA when carrying out a transfer of personal data on the basis of safeguards under Article 46 of UK GDPR.[75] The ICO provides organisations with two permitted approaches: the ICO's approach in the TRA tool (which is focused on the risks to individuals' rights arising from the transfer) or the approach adopted by the EDPB in its Recommendations 01/2020.[76]

4. International Data Transfers – UK's first 'Data Bridge'

In November 2022, the UK Government formalised its first post-Brexit adequacy decision, with the Republic of Korea.[77]

The ‘data bridge’ (the UK Government’s new term for adequacy decisions), which entered into force on 19 December 2022, has a broader scope than the existing EU adequacy decision recognising South Korea.[78]

5. ICO Guidance for Employers

On 12 October 2022, the ICO launched a consultation on its proposed new guidance on monitoring in the workplace.[79] The consultation followed a call for views between August and October 2021. The ICO also published an impact scoping document, outlining some of the potential benefits and costs associated with its proposed guidance.[80]

The ICO’s proposed guidance provides organisations with advice on a number of general issues arising in relation to workplace monitoring, as well as advice and compliance checklists covering a range of specific monitoring scenarios.

The ICO also launched a separate consultation in October on its proposed new guidance for employers handling workers’ health information.[81]

6. Reform of the UK’s cybersecurity regime

In January 2022, the UK Government launched a consultation on proposed legislation to improve the UK’s cyber resilience. The Government’s proposals covered seven policy measures, split across two Pillars: Pillar I (proposals to amend provisions relating to digital service providers) and Pillar II (proposals to future-proof the UK’s NIS Regulations).[82]

In November 2022, the Government confirmed that it would be moving ahead with one of its key proposals, expanding the scope of digital services under the UK’s cybersecurity legislation to include ‘managed services’. This change, which is intended to address growing concerns around supply chain risks, will bring into scope a wide range of providers of technology-related services.[83]

7. AI Action Plan

On 18 July 2022, the UK Government published its AI Action Plan, outlining the steps the Government plans to take to deliver the UK’s National AI Strategy.[84] The Government also published a policy paper setting out its proposed approach to the regulation of AI—in particular, the Government proposes to adopt a context-specific approach, regulating AI based on its use and the impact it has on individuals, groups and businesses within a particular context.

Elsewhere, the ICO launched an updated version of its AI and data protection risk toolkit in May 2022, following comments on the beta version released in 2021. The toolkit is designed to provide support to organisations to help them mitigate risks to individuals resulting from use of AI systems.[85]

B. Switzerland

On 31 August 2022, the Swiss Federal Council confirmed that the revised Federal Act on Data Protection of 1992, alongside two new ordinances on data protection and on data protection certifications, will enter into force on 1 September 2023.[86]

The legislation is adapted and incorporates the responses from the public consultation, including the withdrawal of certain obligations relating to controllers’ obligation to inform when personal data is disclosed, and the terms of the right of access are simplified by removing the requirement to document the reasons for refusing, restricting or delaying access.[87]

With regard to data transfers, the Federal Data Protection and Information Commissioner (“**FDPIC**”) has taken note of the factsheet released by the U.S. regarding the « Data

Privacy Framework » and is analysing it.[88]

C. Russia

The Russian Federation (Russia) has been in a state of war against Ukraine since 24 February 2022. As a consequence, the EDPB adopted a Statement 02/2022 on personal data transfers to the Russian Federation, which recalls that data exporters who transfer personal data to Russia should assess and identify appropriate safeguards and the necessity for supplementary measures to ensure that data subjects are afforded a level of protection that is essentially equivalent to that guaranteed within the EU. [89]

In this regard, the Norwegian Authority also issued a press release[90] encouraging companies which export personal data to Ukraine and Russia to reassess the impact of such transfers. In particular, the Authority advised to reconsider the legal basis of the transfers and recalls that security measures should be reviewed and updated if necessary.

Regarding the legislative framework of Russia, the Federal Service for Supervision of Communications, Information Technology, and Mass Media ("**Roskomnadzor**") announced, on 1 September 2022, the entry into effect of the Federal Law of 14 July 2022 No. 266-FZ on Amending the Federal Law on Personal Data ("**the Amendment Law**") which provides significant changes to the Federal Law of 27 July 2006 No. 152-FZ on Personal Data ("**the Law on Personal Data**"), such as regarding minimum standards applicable to contracts concluded with data subjects for processing of personal data and, the extraterritorial application of the Law on Personal Data in cases where the personal data of Russian subjects is processed by a foreign entity on the basis of an agreement or consent.[91]

In addition, the Federal Law of 14 July 2022 No. 259-FZ on Amendments to the Code of Administrative Offenses of the Russian Federation entered into force on 14 July 2022. In particular, it provides that where a foreign internet operator, with a daily audience of more than 500,000 users, fails to open a branch, representative office, or authorised legal entity in Russia, such operator may be subject to a fine of up to 10% of its annual revenue or, in the case of repeated offences, 20% of its annual revenue.[92]

D. Turkey

The Personal Data Protection Authority ("**KVKK**") published guidance including:

- on 3 January 2022, the second part of its guidance addressing common mistakes in relation to the Law on Protection of Personal Data No., which aims to raise public awareness on some basic issues around the protection of personal data;[93]
- on 11 January 2022, draft guidelines on the Protection of Personal Data for web site operators processing personal data through cookies;[94]
- on 5 August 2022, the banking sector good practices guide on protection of personal data, which provides guidance to data controllers in relation to personal data processing activities carried out by banks, as well as practice examples in this context.[95]

In addition, the Official Gazette of Turkey published, on 19 February 2022, the Regulation on the Protection and Processing of Data at the Social Security Institution ("**SSI**"), to establish the procedures to be followed in the processing of data obtained fully or partially automatically or non-automatically provided that it is a part of any data recording system, within the scope of the duties and relevant authorities.[96]

IV. Developments in Asia-Pacific

A. Australia

As explained in the 2021 and 2022 editions of the International Outlook and Review, the Australian government has undertaken a wholesale review of the Privacy Act 1988 ("**Privacy Act**") commencing in 2020, with a view to implementing significant reforms to the country's privacy regime. The Attorney-General's Department released a discussion paper in October 2021[97] which, along with submissions of the public, ultimately formed the basis of a final report submitted to government in December 2022.[98] Reaching this milestone was scheduled 12 months earlier, however the Attorney General will now consider the report and is expected to publicly release it in the first half of 2023, along with its proposed response.[99]

The 2021 public discussion paper proposed wide-ranging reforms to align Australia's privacy regime more closely with global equivalents (such as the GDPR) in order to reflect recent developments in the digital economy, including to expand the definition of personal information, impose stricter anonymisation requirements on organisations subject to the laws, increase maximum civil penalties for non-compliance, strengthen the rights of individuals to object to the collection and use of disclosure of their information and to require its erasure, in addition to modifying the framework for international data transfers.

As referred to in the 2022 International Outlook and Review, the government's review was initially conducted concurrently with a public consultation process on the exposure draft of the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 ("**Online Privacy Bill**"), which was released in October 2021.[100] The Online Privacy Bill proposed to establish a binding privacy code for social media platforms, data brokerage services and large online platforms, expand the enforcement options available to the regulator, increase the penalties for serious or repeated privacy breaches and significantly broaden the extraterritorial reach of the Privacy Act. While the government ultimately decided not to pursue the Online Privacy Bill, it nonetheless tabled and passed the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 ("**Privacy Enforcement Bill**") in November 2022, amending the Privacy Act.[101] The Privacy Enforcement Bill retained the amendments to the enforcement and penalty regime as well as the expansion of the Privacy Act's extraterritorial reach proposed in the Online Privacy Bill, however it omitted the privacy code. It remains to be seen whether the government will include the code in the broader set of amendments to the Privacy Act which are expected in 2023.

Notably, the Privacy Enforcement Bill was fast-tracked through parliament in the wake of two large scale, and widely publicised, data breaches involving a major domestic telecommunications provider in September 2022,[102] and a major domestic private health insurer in October 2022.[103] These data breaches put privacy reform into the spotlight in Australia in 2022 and it is likely that this will continue to be a focus area for the newly elected government in 2023. Accordingly, we expect the Office of the Australian Information Commissioner ("**OAIC**")—which is tasked with enforcing the provisions of the Privacy Act—to be increasingly focussed on compliance and utilise its broadened suite of enforcement tools.[104]

In this regard, clients should note the revisions to the extraterritorial reach of the Privacy Act in particular. The amendments implemented by the Privacy Enforcement Bill repeal the previous requirement that a foreign organisation must have collected or held personal information in Australia in order for the organisation to have an "Australian link" and render its subsequent acts or practices outside of Australia subject to the Privacy Act. This amendment was widely criticised following the release of the exposure draft of the Privacy Enforcement Bill, primarily on the basis that the amendment potentially results in the application of the Privacy Act to acts or practices of a foreign organisation which do not otherwise have any relevance to Australia or Australian data subjects. The government ultimately determined that these concerns were not sufficient to delay the passing of the Privacy Enforcement Bill but flagged that they would instead consider them as part of the forthcoming set of amendments in 2023.[105]

In addition, as mentioned in the 2022 International Outlook and Review, the US and

Australian governments signed an agreement in December 2021 to facilitate access to electronic data for investigations authorised by the Clarifying Lawful Overseas Use of Data ("**CLOUD**") Act of 2018.[106] This agreement allows authorities from either country to access certain data directly from providers operating in the other jurisdiction to mitigate, detect and investigate serious crimes, including ransomware attacks and terrorism, as well as crimes that sabotage critical infrastructure over the internet. Following a parliamentary inquiry in 2022, the Joint Standing Committee on Treaties recommended that the Australian government ratify the agreement, which will now replace the mutual legal assistance mechanism currently used to access data from such providers.[107]

B. China

The Personal Information Protection Law ("**PIPL**") took effect in 2021[108] but continued to take shape in 2022 as the Cyberspace Administration of China ("**CAC**") issued a wide range of implementing regulations to provide further colour to the law. Notably these regulations included the following:

- ***Cybersecurity Review Measures*** – In January 2022, the CAC (in conjunction with various other Chinese authorities) issued new Cybersecurity Review Measures.[109] The Measures broaden the scope of circumstances triggering a cybersecurity review, including where Critical Information Infrastructure Operators ("**CIIOs**") procure network products or services which affect or may affect China's national security or where internet platform operators carry out data processing activities which affect or may affect China's national security. The Measures also specify the proposed focus and procedures for the conduct of cybersecurity reviews.
- ***Technical Specification for Certification of Cross-Border Transfers of Personal Information*** – In June 2022, the Secretariat of the National Information Security Standardization Technical Committee ("**TC260**") issued the Technical Specification for Certification of Cross-Border Transfers of Personal Information, which was then further revised in December.[110] The Specification supplements Article 38(2) of the PIPL, which provides for one of the mechanisms that data controllers can utilize in order to transfer personal information outside of China between related entities, namely application for certification.
- ***Measures for Security Assessment for Cross-Border Data Transfers*** – In July 2022, the CAC finalized the Measures for Security Assessment for Cross-Border Data Transfers.[111] These Measures supplement Article 40 of the PIPL, which provides that certain CIIOs and data controllers are to store personal information collected and produced within China domestically and must pass a security assessment by the CAC before exporting such personal information overseas. The assessment is only required if a CIIO or data controller meets one of the following criteria and/or thresholds: (i) data controllers exporting "important data"; (ii) CIIOs exporting personal information, or data controllers processing the personal information of 1 million people or more; (iii) data controllers who have exported (A) the personal information of 100.000 people or more or (B) the sensitive personal information of 10.000 people or more, since 1 January of the previous year; or (iv) in any other situations provided for by the CAC. To the extent that they apply, the Measures require data controllers to carry out a self-assessment of data export risks, enter into a data processing agreement with the data recipient and apply to CAC for a security assessment.
- ***Administrative Provisions on Internet Pop-up Push Notifications*** – In September 2022, the CAC finalized the Administrative Provisions on Internet Pop-up Push Notifications.[112] These regulations apply to all owners and operators of operating systems, terminal devices, application software, websites and other such services that provide push notification services in China. The regulations impose restrictions on the inclusion of certain categories of information in push notifications.

The CAC also released a number of draft regulations in 2022, including the following:

- ***Draft Provisions on Standard Contracts for the Export of Personal Information*** – these draft provisions supplement Article 38(3) of the PIPL, which provides that data controllers may use a standard contract in order to transfer personal information outside of China. The draft provisions specify the triggers and conditions for when data controllers may rely on the SCC mechanism, and provide the framework for that mechanism. The draft SCCs contain a standard contract akin to the GDPR and establish requirements for personal information processors as well as overseas recipients, which also include the obligation to carry out an impact assessment of data export risks prior to exporting any personal information.[113]
- ***Mobile Internet Application Program Information Service Management Regulations*** – these draft regulations establish general requirements for app providers to publish privacy notices and deploy technical measures to ensure data security and establish a full-process data security management system, in addition to prohibiting providers from making consent to the collection and processing of users' personal data conditional for use of an app where such collection and processing is not essential for the functioning of the app.[114]

Notwithstanding the legislative activity of the CAC described above, arguably the most significant event to occur in China in 2022 was the fine imposed on a Chinese leading mobile transportation platform. In July, the regulator announced that it had fined the ride hailing platform RMB 8.000.000.000 (approx. US$1.2 billion) for violations of the PIPL, Cyber Security Law and Data Security Law.[115] Following an investigation, the CAC found that the mobile transportation platform had: (i) collected illegal and excessive personal information from users; (ii) failed to clearly and accurately explain the processing purposes of personal information collected; and (iii) failed to fulfil its obligations of cybersecurity, data security, and personal information protection. The severity of the CAC's sanctions suggests that it is now prepared to utilise its broad investigatory and enforcement powers regardless of the potential business impact to companies, particularly those in the technology sector and with overseas (especially U.S.) operations. Further, the classification of the ride hailing platform as a CIIO indicates that the CAC and other Chinese regulators intend to adopt a broad interpretation of the otherwise vaguely defined concept of "critical information infrastructure" under the Cyber Security Law as well as to link mobility data, including location data, with national security.

C. India

In August 2022, the Indian government withdrew the Personal Data Protection ("**PDP**") Bill, which had been pending before parliament since 2019.[116] In its place, India's Ministry of Electronics and Information proposed a new draft bill, titled the Digital Personal Data Protection Bill, 2022 (the "**DPDP**").[117] The DPDP applies extraterritorially to organizations processing personal data outside India if such processing involves the profiling of data principals in India or offering of goods and services to individuals in India. The latest DPDP changes the previous version of the bill, including removing the data localization requirement and changing penalties for non-compliance.

The DPDP removed the previous bill's data localization requirement, and states that "the central government may, after an assessment of such factors as it may consider necessary, notify such countries or territories outside India to which a data fiduciary may transfer personal data". Instead of requiring entities to store data in India, the government may assess different countries' data protection regimes and confirm whether personal data can be transferred to such countries.[118]

The DPDP also changed the previous bill's penalty for noncompliance. The previous bill imposed fines with a cap of 4% of the data fiduciary's worldwide turnover. The DPDP limits fines on a data fiduciary to approximately US$62 million.[119]

The DPDP underwent public consultation up to 2 January 2023 and will now follow the same legislative process as the previous bill.[120]

D. Indonesia

2022 was a landmark year for data protection in Indonesia. In September, the House of Representatives approved the Personal Data Protection Bill, which was then enacted in October as Law No.27 of 2022 on Personal Data Protection ("**PDP Law**").[121] Years in the making, the PDP Law consolidates the rules related to personal data protection in Indonesia and establishes data sovereignty and security as the keystone of Indonesia's data protection regime. Key features of the PDP Law are set out below:

- ***Transitional Period*** – Personal data controllers, personal data processors and other parties relevant to the processing of personal data have up to two years from the date of enactment of the PDP Law to comply with its terms. As is typical in Indonesia, implementing regulations for the PDP Law will follow its enactment and are expected to be issued throughout 2023.
- ***Extraterritorial Application*** – Consistent with the reforms in other international jurisdictions, the PDP Law applies extraterritorially to organisation outside of Indonesia so long as the processing of personal data has legal consequences (i) in Indonesia; or (ii) for personal data subjects of Indonesian citizens outside of Indonesia.
- ***Consent to Processing of Personal Data*** – The PDP Law requires personal data controllers to obtain the valid and explicit consent from personal data subjects for one or more specific purposes which it has informed to those personal data subjects. Such consent can be either written or recorded and personal data controllers must be able to show proof of the data subjects' consent. The request of a personal data controller for consent must also fulfil certain formalities, including that it is made in an understandable and accessible format.
- ***Notification in Corporate Restructuring*** – The PDP Law requires personal data controllers to notify data subjects prior to and after carrying out a merger, spin-off, acquisition, consolidation, or dissolution. However the applicable notification procedures (including the thresholds for their application) will not be defined until the release of the forthcoming implementing regulations.
- ***Obligations of Personal Data Controllers and Processors*** – The PDP Law imposes additional obligations on personal data controllers and personal data processors, including (i) ensuring the accuracy, completeness, and consistency of personal data; (ii) supervising each party that is involved in the personal data processing under the control of the personal data controller; and (iii) recording all personal data processing activities.
- ***Transfer of Personal Data to Outside of Indonesia*** – The PDP Law requires that, where a personal data controller seeks to transfer personal data outside of Indonesia, the personal data controller: (i) obtains prior approval from the data subject; and (ii) ensures that the country of domicile of the personal data controller and/or the personal data processor that receives the transfer of personal data has a personal data protection level that is equal to or higher than those that are regulated under the PDP Law. As above, the practical operation of these overseas transfer rules will be further defined through the forthcoming regulations.
- ***Enforceability of Existing Laws*** – The PDP Law provides that following its enactment, all provisions of laws and regulations governing the protection of personal data in Indonesia shall remain valid, provided that they do not conflict with the provisions of the PDP Law. Hence, the PDP Law will not revoke the previous regulations on personal data in Indonesia including, among others, the MOCI Regulation No. 20/2016.[122]
- ***Sanctions*** – The PDP Law imposes criminal sanctions for certain violations of

prohibitions on the use of personal data, including unlawfully obtaining or collecting, disclosing or using personal data that is not a person's own. Corporations may face fines of up to 2% of their annual revenues, in addition to seizure and/or freezing of the profits or assets derived from the crime and deregistration at an entity level. The PDP Law also provides that members of management (i.e., board of directors), controllers, those giving orders ("*pemberi perintah*") and beneficial owners (among others) may be subject to prison sentences subject to the nature of the violation.

E. Hong Kong

The Personal Data (Privacy) Ordinance ("**PDPO**"), passed in 1995, is one of Asia's longest standing data protection laws. As identified in the 2021 and 2022 editions of the International Outlook and Review, the PDPO was amended in 2021 to combat doxxing acts which intrude on personal data privacy however has not since undergone any substantive amendment.[123]

While the Privacy Commissioner for Personal Data ("**PCPD**") issued two investigation reports against EC Healthcare and Fotomax in November 2022 for respective violations of provisions of the PDPO, it remains to be seen whether this indicates a renewed enforcement focus by the PCPD which has historically been seen as permissive in this space.[124]

F. Japan

The latest amendments to Japan's Act on the Protection of Personal Information ("**APPI**") took effect in April 2022.[125] As a consequence, the APPI now has extraterritorial applicability insofar as it applies to organizations collecting personal data outside Japan if such processing involves offering goods and services to individuals in Japan. The APPI includes, but is not limited to, requirements related to cross border data transfers and data breach notifications.

With respect to cross border data transfers, the APPI requires a business to (i) obtain opt-in consent before transferring personal information outside of Japan (i.e., through email, written or verbal explanations, or website publications) or (ii) execute contracts with foreign third-party processors with contractual safeguards to handle data in accordance with the APPI.

The APPI also now imposes data breach notification requirements on entities. Data breaches involving (i) sensitive data, (ii) data which may result in economic loss (e.g., credit cards), (iii) unjust purposes (e.g., ransomware), or (iv) over 1.000 data subjects must be reported to the Personal Information Protection Commission.

G. New Zealand

As mentioned in the 2022 International Outlook and Review, the New Zealand Privacy Act 2020 ("**NZ Privacy Act**") came into force on 1 December 2020, repealing and replacing an existing 1993 act.[126] In implementing the new act, the New Zealand government sought to modernise the privacy regime in New Zealand and reflect global trends in international privacy standards and the digital economy.

Despite the recommendation of the Office of the Privacy Commissioner in 2021 that "further changes [were] desirable" in response to fast-changing technologies, no amendments have been forthcoming in 2022.[127] The proposed changes are nonetheless slated to broaden the NZ Privacy Act's notification requirements (see below), introduce a right of personal information portability and a right to be forgotten, protect data subjects against the risk of re-identification from de-identified information, limit the harm caused by automated decision making algorithms, increase civil penalties for non-compliance and expand powers of the regulator to require compliance reporting by

organisations subject to the NZ Privacy Act.

Despite this lack of substantive reform, New Zealand's Ministry of Justice released its consultation paper on possible changes to data collection notification requirements in the Privacy Act 2020. In his comments, New Zealand's Privacy Commissioner noted the lack of notification requirements related to indirect collection (i.e., if an agency collects information indirectly from a data subject).[128]

H. Philippines

On 4 February 2021, the National Privacy Commission of the Philippines ("**NPC**") announced the approval of a substitute bill to amend the Data Privacy Act of 2012 ("**PDPA**"). As noted in the 2022 International Outlook and Review, the substitute bill seeks to implement wide-ranging reforms to the Philippines privacy regime, including to redefine "sensitive personal information" to include biometric and genetic data, clarify the extraterritorial application of the PDPA (including in circumstances where an organisation offers goods or services, or monitors the behaviour of individuals within the Philippines or where it has a link with the country), render performance of a contract as a lawful basis for processing of personal information, allow controllers outside of the Philippines to authorise processors within the Philippines to notify the NPC of a data breach, widen the enforcement powers of the NPC and modify the criminal penalties for non-compliance.[129] Despite the substantial passage of time since the NPC approved the substitute bill, it remains before the Senate and is yet to pass into law. In light of the election of the Marcos administration in the intervening period, it is still unclear when this will occur.

The NPC nonetheless introduced Circular No. 2022-01 on the Guidelines on Administrative Fines in June which categorises infractions under the PDPA as "grave", "major" or "other" based on the number of data subjects affected, the frequency of the infractions and the reason for non-compliance. The different categories correspond to the threshold of and basis for calculation of potential fines.[130]

The NPC also announced in March that it is in the process of developing guidelines for the processing of personal and sensitive personal information based on consent, contract, and legitimate interests. The NPC is currently seeking public submissions for this purpose.[131]

I. Singapore

Further amendments to the Personal Data Protection Act 2012 ("**PDPA**") based on the Personal Data Protection (Amendment) Act 2020 (No. 40 of 2020) took effect on 1 October 2022.[132] Notably, these amendments enhance the power of the Personal Data Protection Commission ("**PDPC**") to accept voluntary undertakings as part of its enforcement regime, as well as increasing the financial penalty cap for breaches of the PDPA by organisations with annual local turnover exceeding US$10 million from the previously fixed US$1 million to 10% of the organisation's annual local turnover.

In a case which required a determination as to whether emotional distress is a form of loss or damage, the Singapore Court of Appeal found that the PDPA should be interpreted widely in order to further its purpose of enabling individuals to enforce their rights to protect their personal data. However, the Court imposed limits on this broad interpretation, insofar as it held that the loss of *control* of personal data would not constitute loss or damage for the purposes of the PDPA.[133].

J. South Korea

As explained in the 2022 International Outlook and Review, data protection in South Korea is currently governed by the Personal Information Protection Act ("**PIPA**"),[134] with the Personal Information Protection Commission ("**PIPC**") being the authorised body.

In September 2022, the PIPC imposed its largest ever sanction for violations of the PIPA against an American search engine and social media platform. The regulator fined the digital platforms a total of 100 billion won (about US$78.4 million), alongside issuing corrective orders, following an 18-month inquiry in which it found that the companies had failed to clearly inform users and secure their consent prior to using behavioral data for targeted ads.[135]

The fines were the first time that the PIPC has taken action against digital platforms over their data collection practices, and suggests a renewed enforcement focus by the agency in this area. Indeed consistent with other regulators internationally, the PIPC Chairman Ko Hak-soo indicated in his announcement of the PIPC's policy agenda for 2023[136] that he would ensure that the agency plays a vital role in safely managing privacy in the digital economy. Additional policy goals for 2023 include the inspection of cross-border data-transfer practices of around 5,000 mobile apps in gaming, finance, shopping, education, social media and entertainment, as well as an industry-wide inspection to detect potential privacy risks involving dark patterns, ad tech, virtual platforms, super apps and smart gadgets. The PIPC is also planning to strengthen requirements for global companies to designate their local business operations as legal representatives.

An update to the PIPA which would grant the PIPC the power to impose severe fines on anyone found to have violated the law is also tabled for approval in 2023. If the amendments are pursued, digital platforms could potentially be subject to fines of as much as 3% of the "total annual turnover" for a privacy breach, in contrast to the "relevant turnover" defined under current rules. The legislative proposal was presented in 2022, recently passed the National Policy Committee and is now up for review by the Legislation and Judiciary Committee and a vote in the plenary.

K. Sri Lanka

Sri Lanka's official gazette published the Regulation of Processing of Personal Data (2021) on 25 November 2021 to be considered by the Parliament of Sri Lanka.[137] The Parliament of Sri Lanka has since enacted the Personal Data Protection Act No. 9 of 2022 ("**Sri Lanka PDPA**") which was adopted on 19 March 2022. In line with other international standards, the PDPA applies to all businesses, regardless of size, and requires that the processing of personal information must be for a "specified, explicit and legitimate" purpose. Controllers and processors are also required to implement internal controls and procedures, referred to as the "Data Protection Management Programme". Businesses will only be able to process Sri Lankan personal data abroad if the business is located in a country that has been deemed to have adequate data privacy laws, however, various exceptions to the rule exist including where the data subject has given consent. The Act will enter into force at the start of 2023.

L. Thailand

Thailand's Personal Data Protection Act (the "**PDPA**") took effect on June 1, 2022.[138] The PDPA, initially enacted in May 2019, overcame a delay of three years due to the COVID-19 pandemic and is the first comprehensive data protection regulation in Thailand. The PDPA has extraterritorial applicability, as it applies to organizations collecting personal data outside Thailand if such processing involves offering goods and services to individuals in Thailand. Similar to the GDPR, the PDPA requires a legal basis for the processing of data and details data subject rights (e.g., the right to be informed, right to access, right to rectification, right to erasure, right to opt-out, right to portability, right to complain, and right to withdraw consent). The PDPA's penalty for noncompliance includes an administrative fine up to approximately US$150.000 and a criminal fine up to approximately US$30.000 or imprisonment.

M. Vietnam

As explained in the 2022 International Outlook and Review, the data protection framework

in Vietnam is fragmented, and relevant provisions can be found in numerous laws. In February 2020, however, a draft personal data protection decree ("**Draft PDPD**") was released. The Draft PDPD sets out principles of data protection, including purpose limitation, data security, data subject rights and the regulation of cross-border data transfers, in addition to provisions on obtaining consent of data subjects, the technical measures needed to protect personal data, the creation of a data protection authority and the introduction of penalties for non-compliance, ranging between VDN 50 million to VDN 100 million.

From February to April 2021, the Ministry of Public Security sought public comments on the Draft PDPD with a view to the final decree coming into effect on 1 December 2021. As of the date of this publication, the Draft PDPD is still pending declaration in Vietnam, while a new Decree No. 53/2022/ND-CP ("**Decree 53**")[139] has been issued to provide guidance on the Law on Cyber Security No. 24/2018/QH14 ("**Cybersecurity Law**").[140]

Decree 53, which took effect on 1 October 2022, clarifies some important aspects of the Cybersecurity Law, including the application of the data localisation requirements to Vietnam domiciled entities and foreign enterprises. The criteria under the Cybersecurity Law and Decree 53 together provide that the data localisation requirements only apply to Vietnam domiciled entities that: (i) are service providers in the telecommunications network, internet or providing value added services in cyberspace; and (ii) process the personal data of Vietnam users, data about the relationship of users in Vietnam or data created by users in Vietnam.

Domestic entities to which Decree 53 applies must retain such specified categories of data in Vietnam indefinitely. However, Decree 53 clarifies that foreign entities will only need to store relevant data in Vietnam and establish a local presence where all of the following conditions are met:

- the company operates in a prescribed sector related to the cyberspace, which means, amongst other things, telecom services, services for storing and sharing data in cyberspace, e-commerce and online payment services ("**Specified Services**");
- the company violates Cybersecurity Law in performing the Specified Services;
- the company fails to comply with a notice or request from the Department for Cybersecurity and Prevention of High-Tech Crime ("**DCPHC**"); and
- the DCPHC issues a request for data localisation and local presence establishment.

While Decree 53 is helpful in clarifying aspects of the Cybersecurity Law related to data localisation, it relevantly does not provide for any alternative legal bases for processing personal data nor contain any thresholds for notifiable data breaches—both of which represent gaps in the current legislation.

V. Developments in Africa

A. Kenya

On 21 December 2022, the **Office of the Data Protection Commission** ("**ODPC**") issued a penalty notice of KES 5 million (approx. €38.237) against a mobile manufacturer for failure to comply with an enforcement notice.[141] The mobile manufacturer had made use of the complainant's photograph on its Instagram account without obtaining the data subject's consent. In response, the ODPC issued an order requesting that the company develops a) a policy for compliance with Section 37 of the Data Protection Act 2019—requiring data controllers to obtain consent prior to the use of personal data for commercial purposes—and b) an internal complaints mechanism to address such complaints made by data subjects. The mobile manufacturer failed to comply with the

orders and was fined.

B. Mozambique

On 22 November 2022, the National Institute of Information and Communication Technologies ("**INTIC**") published a draft Cybersecurity Bill. The draft legislation aims to ensure the security of all citizens and institutions by protecting digital networks, information systems and critical infrastructure in cyberspace.[142] The Bill also provides for the creation of the National Cyber Security Council—a body that will work towards the alignment of policies on cybersecurity. The new agency will be chaired by the Minister of Information and Communication Technology.

C. Nigeria

On 4 October 2022, the National Data Protection Bureau ("**NDPB**") released the Draft Data Protection Bill 2022.[143] The Bill affords data subjects a number of rights (similar to those afforded under the GDPR), provides for the designation of data protection officers ("**DPO**") and outlines the legal bases for the processing of personal information. To oversee the enforcement and regulation of the above provisions, the draft legislation creates the Nigerian Data Protection Commission. The maximum fine that can be levied on transgressors is set at NGN 10 million (approx. €23.540) and 2% of the transgressor's annual gross revenue derived from Nigeria in the preceding financial year.

D. Tanzania

On 1 November 2022, Tanzania's legislative body voted in favour of the Personal Information Protection Bill—a notable development considering this is Tanzania's first law on data protection.[144] The Bill will establish a Commission responsible for the protection of personal data. In addition, the Bill introduces a requirement that controllers and processors of personal data be registered with the Commission. On the enforcement side, the Bill provides that the Commission may issue an enforcement notice against a person who has failed to comply with the law. The maximum fine that can be levied against the transgressor is set at TZS 100 million (approx. €41.320). The Ministry of Information, Communication, and Information Technology has not yet announced when the Bill will come into force.

E. Zimbabwe

On 16 November 2022, the Postal and Telecommunications Regulatory Authority of Zimbabwe ("**POTRAZ**") published the Draft Cyber and Data Protection Regulations 2022. The Draft provides for the designation of a DPO in certain cases (e.g., when the data processing is carried out by a public authority or body). Furthermore, the Draft introduces a number of data security provisions, most notable of which is that if a controller decides to rely on a legitimate interest for processing data, a Legitimate Interest Assessment ("**LIA**") must be conducted first, a record of which must be kept in order to demonstrate compliance. As a general overview, the Draft Regulations aim to ensure that data is processed securely and that the appropriate organizational measures are adopted.[145]

VI. Other Developments in the Middle East

A. Israel

On 29 November 2022, the Ministry of Justice published the Draft Privacy Protection Regulations (Provisions Regarding Information Transferred to Israel from the European Economic Area). The draft legislation requires that Israeli data controllers abide by a series of obligations in relation to the handling and processing of personal data transferred from the European Economic Area ("**EEA**") to Israel.[146] Israel was granted adequacy in 2011 (i.e., providing equivalent level of protection as that provided within the EU).[147] Since then, the EU has introduced the GDPR and Israel's status is expected to be

reviewed.

Through the draft legislation, Israel aims to satisfy the EU's demands and retain its status as an adequate country. The new provisions are the following: a) obligation to delete information upon request, b) deletion of excess personal information, c) obligation to maintain accurate personal information and, d) obligation to notify EEA data subjects that their personal information is being processed. It should be noted that the new law will only apply to EEA data subjects. The protection of Israeli data subjects will remain unchanged.

B. Saudi Arabia

On 20 November 2022, the Saudi Data and Artificial Intelligence Authority ("**SDAIA**") published its proposed amendments to the Personal Data Protection Law. The SDAIA has invited the public to express their comments. The draft legislation introduces, inter alia, a) the right to data portability, pursuant to which data subjects may request that their personal data be transferred to another controller, b) an obligation that the controller keeps records of the operations performed on personal data and c) the ability to apply to a competent court for compensation in case one suffers damage as a result of a violation of the Personal Data Protection Law.[148]

On 8 August 2022, the Saudi National Cybersecurity Authority ("**NCA**") launched a programme which aims to develop the cybersecurity sector in the country. Specifically, the programme will look to foster the development of national cybersecurity products, services and solutions.[149]

C. Other Middle East Jurisdictions

On 17 March 2022, the Ministry of Justice, Islamic Affairs and Endowments of Bahrain announced several executive decisions supplementing the Personal Data Protection Law 2018.[150]

On 9 February 2022, Oman enacted its first data protection legislation (Law on the Protection of Personal Data) which is due to come into force on 9 February 2023.[151]

VII. Developments in Latin America and in the Caribbean Area

A. Argentina

On 10 November 2022, the Argentinian data protection authority ("**AAIP**") published a draft bill to update the Personal Data Protection Act, Act No. 25.326 of 2000, following a public consultation on the act during September 2022.[152] In particular, the draft bill includes data minimisation, an obligation of information for the data controller before collection of personal data, the burden on the exporter to demonstrate that the international transfer is carried out in accordance to the draft bill. A web form has also been set up for the registration of data controllers who do not reside in Argentina to enable Argentinian data subjects to exercise their data subject rights before the foreign data controllers.[153]

B. Brazil

On 8 November 2022, the Brazilian Data Protection Authority ("**ANDP**") approved its regulatory agenda for 2023-2024 which includes as priorities the rights of children and adolescents whose personal data is being processed and the establishment of criteria to guide the calculation of fines.[154]

The ANPD also published Guidance on Cookies and Personal Data Protection, which outlines requirements and best practices associated with cookie policies and cookie banners.[155]

On 23 August 2022, Brazil's National Consumer Secretariat ("**Senacon**") issued a fine against a U.S. social media company amounting to BRL 6.6 million (approx. €1,290,000) for the unlawful sharing of personal data of Brazilian citizens.[156]

It should also be noted that an amendment included the protection of personal data as a fundamental right and guarantee in the Brazilian Constitution.[157]

C. Chile

On 7 June 2022, the Information Security Incident Response Team ("**CSIRT**") released guidance for organisations on cyberattacks and the best practice capabilities to have in place.[158]

D. Mexico

On 31 May 2022, the National Institute for Access to Information and Protection of Personal Data ("**INAI**") released its Recommendations for the Processing of Personal Data derived from the Use of Artificial Intelligence.[159]

E. Peru

On 25 October 2022, the National Authority for the Protection of Personal Data ("**ANPD**") approved the "Guide for the Implementation of Model Contractual Clauses for the International Transfer of Personal Data" which aims to ensure the compliance of international data transfers.[160]

F. Uruguay

On 3 November 2022, the Official Information Center of Uruguay ("**IMPO**") published the Law No. 20075 of 20 October 2022 reforming the country's data protection law. The reforms intend to increase transparency in data processing, especially when algorithms are utilised for decision-making.[161]

G. Developments in Other Latin American and Caribbean Jurisdictions

On 4 August 2022, the Congress of the Republic of Guatemala voted in favour of the Law on Prevention and Protection Against Cybercrime which criminalizes cybercrime and intends to protect Guatemalans from the unlawful use of their personal data.[162]

On 22 May 2022, the Presidency of Peru's Council of Ministers ("**PCM**") announced the establishment of the National Centre for Digital Security. The agency will work with both public and private sector companies to identify, detect and respond to digital security incidents in the country.[163]

---

[1] *See* Irish Supervisory Authority decision.

[2] *See* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R2065.

[3] *See* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925.

[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=COM%3A2022%3A68%3AFIN.

[6] *See* https://www.cnil.fr/en/european-strategy-data-cnil-and-its-counterparts-comment-data-

governance-act-and-data-act.

[7] *See* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555.

[8] *See* https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.

[9] *See* https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.

[10] *See* CAC decision.

[11] *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.

[12] *See* https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7631.

[13] *Id.*

[14] *See* https://www.cnil.fr/en/transfer-data-outside-eu-old-standard-contractual-clauses-scc-are-no-longer-valid#:~:text=A%20transition%20period%20of%20three,%E2%80%9Cold%E2%80%9D%20standard%20contractual%20clauses.

[15] *See* https://commission.europa.eu/select-language?destination=/node/9; https://commission.europa.eu/system/files/2022-05/questions_answers_on_sccs_en.pdf.

[16] *Id.*

[17] *See* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/?_sm_au_=iHVNDSq41vR3q5QMFcVTvKQkcK8MG.

[18] *See* https://edpb.europa.eu/system/files/2022-03/edpb_guidelines_codes_conduct_transfers_after_public_consultation_en_1.pdf.

[19] *See* https://edpb.europa.eu/system/files/2022-11/edpb_recommendations_20221_bcr-c_referentialapplicationform_en.pdf.

[20] *See*, e.g., the UK Supervisory Authority published an update to its guidance on international transfers, including a new section on transfer risk assessments (TRAs) and a TRA tool. The Danish Authority released guidance on Cloud service usage which provides specific recommendations for transferring data to third countries like the U.S. and examples of how data transfers should be implemented. The Hamburg Commissioner for Data Protection and Freedom of Information issued a press release regarding the impact of the Executive Order signed by President Biden to implement the EU-U.S. Data Privacy Framework. 10/07/2022. The Berlin Supervisory Authority issued guidance to outline the requirements for cross-border data transfers and clarifies the current legal situation regarding international data transfers while examining the U.S. surveillance framework, the *Schrems II* ruling and their implications.

[21] *See*, e.g., the French CNIL ordered companies using Google Analytics to comply with the GDPR and if needed to stop using this tool. The Liechtenstein Authority issued a press release, recommending website operators to deactivate Google Analytics and implement alternative tools. The Austrian Supervisory Authority reaffirmed that Google Analytics

cannot be used in accordance with the GDPR. The Italian Supervisory Authority issued a reprimand against a website operator, to be followed by others and banned the use of Google Analytics. The Danish Supervisory Authority issued a decision against a company using the analytics tool of an American company.

[22] *See* https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/google-analytics-et-transferts-de-donnees-comment-mettre-son-outil-de-mesure-daudience-en-conformite.

[23] *See* https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/questions-reponses-sur-les-mises-en-demeure-de-la-cnil-concernant-lutilisation-de-google-analytics.

[24] *See* Spanish Supervisory Authority decision.

[25] *See* Danish Supervisory Authority decision.

[26] *See* Regional Court of Munich decision.

[27] *See* Thuringia Data Protection Authority recommendation.

[28] *See* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555.

[29] *Id.*

[30] *See* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R0868.

[31] *See* https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained.

[32] *See* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2022:277:FULL&from=EN.

[33] *See* https://ec.europa.eu/commission/presscorner/detail/en/IP_22_6906.

[34] *See* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925; https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2349.

[35] *Id.*

[36] *See* https://eur-lex.europa.eu/eli/reg/2022/2554/oj.

[37] *See* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN.

[38] *See* https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113.

[39] *See* https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22022-proposal-european_en.

[40] *See* https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act; https://digital-strategy.ec.europa.eu/en/news/new-eu-cybersecurity-rules-ensure-more-secure-hardware-and-software-products.

[41] *Id.*

[42] *Id.*

[43]
See https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF.

[44]
See https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/#:~:text=The%20Council%20has%20adopted%20its,fundamental%20rights%20and%20Union%20values.

[45]
See https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf.

[46]
See
https://edpb.europa.eu/system/files/2022-03/guidelines_202202_on_the_application_of_article_60_gdpr_en.pdf.

[47]
See
https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf.

[48]
See
https://edpb.europa.eu/system/files/2022-05/edpb_guidelines_042022_calculationofadministrativefines_en.pdf.

[49]
See
https://edpb.europa.eu/system/files/2022-06/edpb_guidelines_202206_on_the_practical_implementation_of_amicable_settlements_en.pdf.

[50]
See
https://edpb.europa.eu/system/files/2022-06/edpb_guidelines_202207_certificationfortransfers_en_1.pdf.

[51] *See*

https://edpb.europa.eu/system/files/2022-10/edpb_guidelines_202208_identifyinglsa_targetedupdate_en.pdf.

[52] *See* https://edpb.europa.eu/system/files/2022-10/edpb_guidelines_202209_personal_data_breach_notification_targetedupdate_en.pdf.

[53]
See
https://edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202203_europeanhealthdataspace_en.pdf.

[54]
See
https://edpb.europa.eu/system/files/2022-07/edpb_document_20220712_selectionofstrategiccases_en.pdf.

[55]
See https://eur-lex.europa.eu/legal-

content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=FR.

[56] *See* French Supervisory Authority decision.

[57] *See* French Conseil d'Etat decision.

[58] *See* Irish Supervisory Authority decision.

[59] *See* Italian Supervisory Authority decision.

[60] *See* UK Supervisory Authority decision.

[61] *See* Hellenic Supervisory Authority decision.

[62] *See* French Supervisory Authority decision.

[63] *See* Irish Supervisory Authority decision.

[64] *See* EDPB binding decision.

[65] *See* Irish Supervisory Authority decision.

[66] *See* French Supervisory Authority decision.

[67] *See* Irish Supervisory Authority decision.

[68] *See* https://bills.parliament.uk/bills/3322.

[69] *See* https://publications.parliament.uk/pa/bills/cbill/58-03/0143/en/220143en.pdf.

[70] *Id.*

[71] *See* https://hansard.parliament.uk/commons/2022-09-05/debates/FB4997E6-14A2-4F25-9472-E2EE7F00778A/BusinessStatement.

[72] *See* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/.

[73] *See* https://ico.org.uk/media/for-organisations/documents/4019534/scc-transitional-provisions.pdf.

[74] *See* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/transfer-risk-assessments/#TRA-tool.

[75] *See* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/.

[76] *See* https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en.

[77]

See https://www.gov.uk/government/news/uk-finalises-landmark-data-decision-with-south-korea-to-help-unlock-millions-in-economic-growth.

[78] *Id.*

[79] *See* https://ico.org.uk/media/about-the-ico/consultations/4021868/draft-monitoring-at-work-20221011.pdf.

[80] *See* https://ico.org.uk/media/about-the-ico/consultations/4021867/monitoring-at-work-impact-scoping-20221011.pdf.

[81] *See* https://ico.org.uk/media/about-the-ico/consultations/4022057/employment-practices-workers-health-draft.pdf.

[82] *See* https://www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience.

[83] *See* https://www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience/proposal-for-legislation-to-improve-the-uks-cyber-resilience.

[84] *See* https://www.gov.uk/government/publications/national-ai-strategy-ai-action-plan#:~:text=The%20AI%20Action%20Plan%20outlines,position%20as%20an%20AI%20leader.

[85] *See* https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/ai-and-data-protection-risk-toolkit/.

[86] *See* https://www.fedlex.admin.ch/eli/fga/2020/1998/fr; https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-90134.html.

[87] *Id.*

[88] *See* https://www.edoeb.admin.ch/edoeb/en/home/latest-news/aktuell_news.html.

[89] *See* https://edpb.europa.eu/system/files/2022-07/edpb_statement_20220712_transferstorussia_en.pdf.

[90] *See* https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2022/overforing-av-data-til-russland-og-ukraina/.

[91] *See* https://rkn.gov.ru/news/rsoc/news74484.htm; http://publication.pravo.gov.ru/Document/View/0001202207140080.

[92] *See* http://publication.pravo.gov.ru/Document/View/0001202207140022.

[93] *See* https://kvkk.gov.tr/SharedFolderServer/CMSFiles/d077b665-66b6-4615-975a-249f93e084ba.pdf.

[94] *See* https://kvkk.gov.tr/SharedFolderServer/CMSFiles/fb193dbb-b159-4221-8a7b-3addc083d33f.pdf.

[95] *See* https://kvkk.gov.tr/SharedFolderServer/CMSFiles/12236bad-8de1-4c94-aad6-bb93f53271fb.pdf.

[96] *See* https://www.resmigazete.gov.tr/eskiler/2022/02/20220219-4.htm.

[97] *See* https://www.oaic.gov.au/engage-with-us/submissions/privacy-act-review-discussion-paper-submission.

[98] *See* https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/.

[99] *See* https://www.innovationaus.com/privacy-act-review-complete-after-three-years/.

[100] *See* https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/.

[101] *See* https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd2223a/23bd030.

[102] *See* https://www.oaic.gov.au/updates/news-and-media/oaic-opens-investigation-into-medibank-over-data-breach.

[103] *See* https://www.oaic.gov.au/updates/news-and-media/oaic-opens-investigation-into-optus-over-data-breach.

[104] *See* https://www.oaic.gov.au/updates/news-and-media/oaic-welcomes-passing-of-privacy-bill.

[105] *See* https://parlinfo.aph.gov.au/parlInfo/download/committees/reportsen/025001/toc_pdf/PrivacyLegislationAmendment(EnforcementandOtherMeasures)Bill2022[Provisions].pdf;fileType=application%2Fpdf.

[106] *See* https://www.justice.gov/opa/pr/united-states-and-australia-enter-cloud-act-agreement-facilitate-investigations-serious-crime.

[107] *See* https://www.aph.gov.au/About_Parliament/House_of_Representatives/About_the_House_News/Media_Releases/Treaties_Committee_supports_ratification_of_CLOUD_Act_Agreement.

[108] *See an unofficial translation of the PIPL available here and the Mandarin version of the PIPL available here.*

[109] *See* http://www.cac.gov.cn/2022-01/04/c_1642894602182845.htm.

[110] *See* https://www.china-briefing.com/news/new-certification-standards-for-cross-border-processing-of-personal-information-offer-more-clarity-for-foreign-companies/.

[111] *See*

https://www.china-briefing.com/news/cross-border-data-transfer-new-measures-offer-clarification-on-security-review/.

[112] *See* http://www.pkulaw.cn/fulltext_form.aspx?Db=chl&Gid=5134466.

[113] *See* https://www.china-briefing.com/news/cross-border-data-transfer-new-provisions-clarify-contract-procedure-for-personal-information-export/.

[114] *See* https://digichina.stanford.edu/work/translation-mobile-internet-application-program-information-service-management-regulations-opinion-seeking-draft-jan-2022/.

[115] *See* CAC decision.

[116] *See* http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

[117] *See* https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Protection%20Bill%2C%202022_0.pdf.

[118] *Id.*

[119] *Id.*

[120] *See* https://pib.gov.in/PressReleasePage.aspx?PRID=1886126.

[121] *See the final bill (in Bahasa):* https://www.dpr.go.id/dokakd/dokumen/K1-RJ-20220920-123712-3183.pdf.

[122] *See* http://makna.co/wp-content/uploads/2018/01/MOCI-Regulation-No-20-of-2016-Makna-Eng.pdf.

[123] *See* https://www.gld.gov.hk/egazette/pdf/20212540/es12021254032.pdf.

[124] *See* https://www.pcpd.org.hk/english/news_events/media_statements/press_20221114.html#:~:text=The%20Office%20of%20the%20Privacy,Limited%20(Fotomax).

[125] *See* https://www.ppc.go.jp/personalinfo/legal/kaiseihogohou/.

[126] *See* https://www.natlawreview.com/article/less-two-weeks-to-go-new-zealand-privacy-act-commences-1-december-2020.

[127] *See* https://www.privacy.org.nz/publications/reports-to-parliament-and-government/2020-briefing-to-the-incoming-minister-of-justice/.

[128] *See* https://www.justice.govt.nz/justice-sector-policy/key-initiatives/broadening-the-privacy-acts-notification-rules/.

[129] *See* https://www.privacy.gov.ph/2021/06/a-stronger-data-privacy-law-sought-in-proposed-amendments/.

[130] *See* https://www.privacy.gov.ph/wp-content/uploads/2022/08/NPC-CIRCULAR-NO.-2022-01-GUIDELINES-ON-ADMINISTRATIVE-FINES-dated-08-AUGUST-2022-w-SGD.pdf.

[131] *See*

https://www.privacy.gov.ph/2022/03/guidelines-on-the-lawful-processing-of-personal-and-or-sensitive-personal-information-based-on-consent-contract-and-or-legitimate-interests/.

[132] *See* https://www.pdpc.gov.sg/news-and-events/announcements/2022/09/amendments-to-enforcement-under-the-personal-data-protection-act-in-updated-advisory-guidelines-and-guide.

[133] *See*Reed, Michael v Bellingham, Alex (Attorney-General, intervener) [2022] SGCA 60.

[134] *See* https://www.pipc.go.kr/cmt/main/english.do.

[135] *See* PIPC Decision.

[136] *Id.*

[137] *See* http://documents.gov.lk/files/bill/2021/11/152-2021_E.pdf.

[138] *See* https://cyrilla.org/es/entity/sl9175g71u?page=1.

[139] *See* https://lawnet.vn/en/vb/Decree-53-2022-ND-CP-elaborating-the-Law-on-cybersecurity-of-Vietnam-80D86.html.

[140] *See* https://www.economica.vn/Content/files/LAW%20%26%20REG/Law%20on%20Cyber%20Security?%202018.pdf.

[141] *See* ODPC Decision.

[142] *See* https://www.intic.gov.mz/wp-content/uploads/2022/11/Proposta-de-Lei-de-Seguranca-Cibernetica?-assinado.pdf.

[143] *See* https://ndpb.gov.ng/Files/Nigeria_Data_Protection_Bill.pdf.

[144] *See* http://www.parliament.go.tz/polis/uploads/bills/1664436755-document%20(38).pdf.

[145] *See* https://www.potraz.gov.zw/wp-content/uploads/2022/11/Draft-Cyber-and-Data-Protection-Regulations-.pdf.

[146] *See* Draft legislation.

[147] *See* https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:027:0039:0042:EN:PDF.

[148] *See* https://istitlaa.ncc.gov.sa/en/Transportation/NDMO/PDPL22/Pages/default.aspx.

[149] *See* https://nca.gov.sa/en/news?item=234.

[150] *See for instance, the Data Subject Rights Decision only available in Arabic*: http://www.pdp.gov.bh/assets/pdf/executive-decisions/rights_of_the_data_subject.pdf.

[151] *See* https://omaninfo.om/topics/85/show/413540.

[152] *See* https://www.argentina.gob.ar/noticias/presentacion-del-proyecto-de-ley-de-proteccion-de-datos-personales.

[153] *See* https://www.argentina.gob.ar/noticias/registro-de-bases-de-datos-personales-para-responsables-extranjeros.

[154] *See* https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-agenda-regulatoria-2023-2024.

[155] *See* https://www.gov.br/anpd/pt-br/assuntos/noticias-periodo-eleitoral/anpd-lanca-guia-orientativo-201ccookies-e-protecao-de-dados-pessoais201d.

[156] *See* Senacom decision.

[157] *See* https://www.camara.leg.br/noticias/850028-promulgada-pec-que-inclui-a-protecao-de-dados-pessoais-entre-direitos-fundamentais-do-cidadao/.

[158] *See* https://www.ciberseguridad.gob.cl/recomendaciones/capacidades-ciberataque/.

[159] *See* https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/RecomendacionesPDP-IA.pdf.

[160] *See* https://www.gob.pe/institucion/minjus/noticias/663844-peru-aprueba-guia-de-implementacion-para-la-transferencia-internacional-de-datos-personales-en-linea-con-estandares-internacionales.

[161] *See* https://www.impo.com.uy/bases/leyes/20075-2022/62.

[162] *See* https://www.congreso.gob.gt/noticias_congreso/8867/2022/4#gsc.tab=0.

[163] *See* https://www.gob.pe/institucion/pcm/noticias/608641-pcm-anuncia-creacion-de-unidad-funcional-de-confianza-digital-para-fortalecer-estrategia-de-prevencion-y-mitigacion-de-riesgos-digitales.

The following Gibson Dunn lawyers assisted in the preparation of this article: Ahmed Baladi, Vera Lukic, Joel Harrison, Connell O'Neill, Clémence Pugnet, Roxane Chrétien, Thomas Baculard, Anastasia Katsari, Nick Hay, and Jocelyn Shih.

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 member of the firm's Privacy, Cybersecurity & Data Innovation practice group:

Europe Ahmed Baladi – Co-Chair, PCDI Practice, Paris (+33 (0) 1 56 43 13 00, abaladi@gibsondunn.com) Kai Gesing – Munich (+49 89 189 33-180, kgesing@gibsondunn.com) Joel Harrison – London (+44(0) 20 7071 4289, jharrison@gibsondunn.com) Vera Lukic – Paris (+33 (0) 1 56 43 13 00, vlukic@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, PCDI Practice, Palo Alto (+1 650-849-5327, aberinger@gibsondunn.com) Jane C. Horvath – Co-Chair, PCDI Practice, Washington, D.C. (+1 202-955-8505, jhorvath@gibsondunn.com) Alexander H. Southwell – Co-Chair, PCDI Practice, New York (+1 212-351-3981, asouthwell@gibsondunn.com) Matthew Benjamin – New York (+1 212-351-4079, mbenjamin@gibsondunn.com) Ryan T. Bergsieker – Denver (+1 303-298-5774, rbergsieker@gibsondunn.com) David P. Burns – Washington, D.C. (+1 202-887-3786, dburns@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) Nicola T. Hanna – Los Angeles (+1 213-229-7269, nhanna@gibsondunn.com) Howard S. Hogan –

Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com) Kristin A. Linsley – San Francisco (+1 415-393-8395, klinsley@gibsondunn.com) Vivek Mohan – Palo Alto (+1 650-849-5345, vmohan@gibsondunn.com) Karl G. Nelson – Dallas (+1 214-698-3203, knelson@gibsondunn.com) Rosemarie T. Ring – San Francisco (+1 415-393-8247, rring@gibsondunn.com) Ashley Rogers – Dallas (+1 214-698-3316, arogers@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) Michael Li-Ming Wong – San Francisco/Palo Alto (+1 415-393-8333/+1 650-849-5393, mwong@gibsondunn.com) Debra Wong Yang – Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)

Related Capabilities

Privacy, Cybersecurity, and Data Innovation