GIBSON DUNN

January 31, 2022

INTERNATIONAL CYBERSECURITY AND DATA PRIVACY OUTLOOK AND REVIEW – 2022

To Our Clients and Friends:

For the fourth consecutive year, and complementing the publication of Gibson Dunn's upcoming tenth annual U.S. Cybersecurity and Data Privacy Outlook and Review, we offer this separate International Outlook and Review. As every year, this Outlook and Review provides an overview of past and upcoming developments related to global privacy and cybersecurity laws.

2021 saw an increasing number of data protection bills and laws passed across numerous international jurisdictions. Notably, China, the UAE, Brazil, Russia and Switzerland, among others, passed new laws, amendments or implementing regulations paving the way for a new round of significant data privacy regimes. It is expected that international authorities will make full use of their new powers in order to apply and enforce their respective data protection legislation in the near future.

In the European Union ("**EU**"), there were a significant number of developments in the evolution of the data protection and cybersecurity landscape:

- In the aftermath of the *Schrems II* ruling, the EDPB adopted a series of Recommendations and Guidelines in order to clarify the regime and rules applicable to data transfers to the U.S. and other jurisdictions that do not benefit from an adequacy decision, as well as on the territorial scope of the General Data Protection Regulation ("**GDPR**"). Furthermore, the European Commission adopted new sets of Standard Contract Clauses ("**SCCs**") that must be used as of 27 September 2021 for new contractual arrangements and apply to existing contractual arrangements by 27 December 2022.

- Further to the three-year review of the e-Privacy Regulation Bill by the EU Member States, negotiations between the Council, the European Parliament and the European Commission commenced for its finalisation and adoption, which is due to replace the 20-year-old e-Privacy Directive.

- EU lawmakers have also made progress on the adoption of the revised Network Infrastructure Security Directive ("**NIS2 Directive**"), which is due to replace the current NIS Directive by expanding its scope and seeking to harmonise further this sector across all levels (including sanctions).

- EU supervisory authorities continued to apply and enforce the GDPR vigorously, imposing record-setting fines and making full use of EU law instruments to achieve a harmonised approach.

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. Aftermath of the *Schrems II* Ruling

As we indicated in the 2021 International Outlook and Review, on 16 July 2020, the so-called ***Schrems II* ruling** of the Court of Justice of the EU ("**CJEU**") struck down the EU-U.S. Privacy Shield, which numerous companies had relied upon to transfer personal data from the EU to the U.S. Despite this, the CJEU also ruled that the SCCs approved by the European Commission, another mechanism used by an even higher number of companies to transfer personal data outside of the EU, remained valid subject to certain caveats.[1]

Further to the *Schrems II* ruling, organisations transferring personal data to a third country must verify, on a case-by-case basis, if there is anything in the law and practice of the third country which may impinge on the appropriate safeguards of the transfer tools (a "**Risk Assessment**"). If the law and practice of the third country do impinge the transfer tools safeguards, the organisations are required to implement supplementary measures to ensure an equivalent level of protection.

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

- **Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data**,[2] which provide guidance to help organisations conduct their Risk Assessment and determine which supplementary measures should be implemented;

- **Recommendations 02/2020 on the European Essential Guarantees for surveillance measures adopted by the EDPB**,[3] which clarify the elements that organisations are required to take into account when assessing the law of a third country dealing with access to data by public authorities for the purpose of surveillance.

In parallel, on 4 June 2021, the European Commission adopted **new SCCs** to cover data transfers among controllers and processors from the European Economic Area ("**EEA**") to third countries not recognised by the European Commission as ensuring an adequate level of protection for personal data.[4] These new set of SCCs replace the old SCCs adopted in 2001 and 2010 under the Data Protection Directive 95/46/EC ("**e-Privacy Directive**"), and take into account the conclusions of the CJEU in *Schrems II*. Since 27 September 2021, it is no longer possible to execute the old SCCs and, as of 27 December 2022, existing contracts will need to have been replaced or amended to incorporate the new SCCs.

The EDPB also adopted the **Guidelines 04/2021 on codes of conduct as tools for transfers**[5], the **Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on**

international transfers as per Chapter V of the GDPR[6], each for public consultation. The latter Guidelines aim to clarify the territorial scope of the GDPR and the provisions on international transfers, to assist controllers and processors to determine whether a particular data processing activity falls directly under the GDPR, or should be covered by a legal data transfer mechanism to provide adequate safeguards.

In light of these developments, several Member State **supervisory authorities issued statements and guidance** in relation to matters concerning international data transfers:[7]

- the Austrian Data Protection Authority ruled that the provider of a website using Google Analytics was illegally transferring data to the U.S. considering that Google, as an electronic communication service provider, is subject to U.S. surveillance and that the safeguards provided were insufficient to prevent U.S. intelligence from accessing the data;

- the Italian Garante[8] fined a Milanese university €200,000 in relation to the transfer of personal data to the U.S. on the basis of the SCCs due to the lack of Risk Assessment and insufficient encryption measures;

- the Belgian *Conseil d'Etat*[9] decided not to suspend a transfer of personal data to the U.S. since it could not exclude that encryption with separate key management can constitute a sufficient supplementary measure in this context;

- in Germany, the Bavarian BayLDA[10] considered a data transfer as being unlawful due to the lack of Risk Assessment;

- the Portuguese CNPD[11] ordered a controller to suspend within 12 hours any international transfers to the U.S. or other third countries without an adequate level of protection; and

- the French *Conseil d'Etat*[12] decided not to suspend transfers of personal data to the U.S. in view of the safeguards implemented by the controller.

2. Adequacy decisions

On 28 June 2021, the European Commission adopted two **adequacy decisions for the United Kingdom**,[13] under the GDPR and the Law Enforcement Directive. These decisions will allow personal data to flow freely from the EU to the UK without the need for additional tools or authorisations. The adequacy findings include a 'sunset clause', which means that the decisions will automatically expire four years after their entry into force. It is likely that the decisions will only be renewed if the UK continues to ensure an adequate level of data protection of personal data.

On 17 December 2021, the European Commission also adopted the **South Korea adequacy decision**,[14] making it possible for personal data to be transferred safely from the EU to the Republic of Korea. With this decision, the Commission guarantees that the South Korean legislation on data protection, combined with the additional safeguards implemented in the country, ensure an adequate level of protection for EU data subjects' personal data.

B. Proposed E-Privacy Regulation and Cookies and Telemarketing Enforcement

As we indicated was likely in the 2021 International Outlook and Review, the e-Privacy Regulation, which was proposed by the European Commission in 2017 to update laws applicable to telecoms, digital and online data processing, was not adopted in 2021.

In 2021, the Council, the European Parliament and the European Commission initiated joint discussions for the adoption of the e-Privacy Regulation. Although the co-legislators failed to find common ground, the situation does not look as dim as in 2020 and 2021. Legislators and industry experts are confident that the final Regulation will be adopted in 2022 or 2023.[15]

Relatedly, European e-privacy laws have continued to be the object of enforcement by EU data protection authorities. As explained further in Section I.E below, in 2021, the Luxemburg, French and Spanish supervisory authorities, among others, imposed significant fines on companies for e-privacy violations (e.g., setting of cookies, the use of online targeted advertising and the use of telemarketing, without consent).

C. Proposed Network Information Security ("NIS2") Directive Proposal

As explained in past iterations of the International Outlook and Review, the Network and Information Security ("**NIS**") Directive, the first piece of EU-wide legislation on cybersecurity, had the specific aim of achieving a high common level of cybersecurity across the Member States.

While the NIS Directive increased the Member States' cybersecurity capabilities, its implementation proved difficult and resulted in a patchwork of national legislations across the EU. To respond to the growth of digitalisation and cyber-attacks, on 16 December 2020, the European Commission submitted the NIS2 Directive Proposal to replace the NIS Directive. The NIS2 Directive Proposal aims to strengthen the security requirements, address the security of supply chains, streamline reporting obligations and introduce more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the EU. The NIS2 Directive Proposal will also have a broader scope of application, effectively requiring more entities and sectors to take the prescribed measures in relation to cybersecurity.

Further to the Council discussions, the European Parliament adopted its report on 28 October 2021, leading to interinstitutional negotiations with the European Commission.[16] It is expected that the NIS2 Directive will be effectively adopted in 2022 or in 2023.

D. EDPB Guidance

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

- **Guidelines 06/2020 on the interplay between the second Payment Services Directive (PSD2) and the GDPR**,[17] which notably address lawful grounds for further processing under the PSD2;

- **Guidelines 07/2020 on the concepts of controller and processor in the GDPR**,[18] which aim to clarify these concepts and the consequences of attributing these roles to entities that collect and process personal data;

- **Guidelines 08/2020 on the targeting of social media users**,[19] which provide an overview of the main parties and the targeting mechanisms involved in such processing, as well as the related GDPR requirements;

- **Guidelines 10/2020 on restrictions under Article 23 GDPR**,[20] which address the grounds for restricting data subjects' rights, including for national security and public defence, and for objectives of general public interest; and

- **Guidelines 01/2021 on Examples regarding Data Breach Notification**,[21]which aim to assist data controllers in determining how to handle data breaches and what factors to consider during a risk assessment.

The EDPB also issued its Strategy 2021-2023,[22] as well as its Work Program 2021/2022,[23] notably announcing awaited Guidelines on, *inter alia*, legitimate interest, blockchain and the calculation of administrative fines.

E. Enforcement by Supervisory Authorities

In 2021, the GDPR and the e-Privacy Directive continued to be applied and enforced by EU Member State supervisory authorities. As explained in previous issues of our Outlook and Review, the GDPR put in place a one-stop shop mechanism to enable lead supervisory authorities of one Member State to adopt decisions and impose fines for EU-wide GDPR violations resulting from cross-border data processing activities.

On 15 June 2021, the CJEU generally upheld and confirmed the status of lead supervisory authorities as "sole interlocutors" of controllers and processors that process personal data cross-border within the EU.[24] Other supervisory authorities cannot therefore initiate any action, administrative or in court, that runs in parallel to that of the lead supervisory authority, except in exceptional circumstances foreseen by the GDPR (e.g., in urgency procedures under Article 66).

The GDPR's jurisdictional rules were also addressed in another matter before the supervisory authority in France. In 2016, the French data protection authority ("**CNIL**") had initiated investigations against the EU operations of a U.S. tech company regarding particularly its data sharing activities with the U.S. parent company. Among the alleged grievances being investigated, the CNIL considered that such data sharing was undertaken without appropriate legal basis. However, one of the key procedural issues being disputed was to determine whether the CNIL still had jurisdiction over a case initiated prior to the GDPR, but which continued after the GDPR became applicable in 2018 and after the U.S. tech company set up an EU establishment in charge of its processing activities in the same year. The CNIL eventually held in 2021 that it did not have jurisdiction on this case and did not sanction the U.S. tech company.

On 16 July 2021, the **Luxembourg CNPD** imposed a record-breaking **€746 million fine** on an e-commerce and online services corporation and required the company to remedy the instances of non-compliance within six months, with a penalty of €746,000 per day of delay.[25] According to the plaintiff, La Quadrature du Net, the company was processing personal data for targeted advertising purposes without a valid legal basis. The sanction has since been partially suspended by a local administrative court.[26]

On 2 September 2021, the **Irish Data Protection Commission ("DPC")** imposed a fine of **€225 million** on online messaging service provider for allegedly failing to meet its transparency obligations under the GDPR. Given that the company's data processing activities were cross-border, the DPC's draft decision was reviewed by other relevant supervisory authorities, as required by the cooperation and consistency mechanism under the GDPR.

On 31 December 2021, the **French CNIL** imposed a **€150 million fine** on Google (€90 million for Google LLC and €60 million for Google Ireland Ltd), as well as a **€60 million fine** on a social network service[27], on the basis of the e-Privacy Directive, for allegedly not enabling users to refuse cookies as easily as to accept them. The CNIL also summoned the companies, in both cases, to bring their practices in compliance with the e-Privacy Directive within three months, with a penalty of €100,000 per day of delay.

On 25 May 2021, the **German Competition Authority ("Bundeskartellamt")** opened proceedings under Germany's 2021 GWB Digitalization Act against Google Germany GmbH, Google Ireland Ltd., Dublin, Ireland, and Alphabet Inc., USA, reviewing Google's data processing terms and cross-service data processing. Subsequently, on 30 December 2021, it took a decision determining that Google has a paramount significance for competition across markets which is a prerequisite for the further investigation under the new law. Of note, the German Bundeskartellamt is not a supervisory authority under the GDPR, but is an active enforcer in the digital economy – including at the interface to the processing of personal data under the GDPR.

In addition, throughout 2021, **several European Supervisory Authorities** issued fines around **€5-10 million**, including for unlawful employee surveillance[28] or marketing calls[29] and lack of valid consent for the processing of personal data.[30]

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

A. UK

In the UK, the Information Commissioner's Office ("**ICO**") has continued to undertake efforts to enforce the UK GDPR and the Data Protection Act 2018. Notably, in 2021, it announced its **provisional intent to fine Clearview AI, Inc. £17 million**[31] for its processing of biometric data scraped from the internet, and issued a provisional notice to stop further processing and delete the personal data of individuals in the UK. Throughout the year, the ICO also imposed fines of a lower amount to corporations and local businesses for their failure to apply data protection and e-privacy laws.[32]

In addition to its enforcement action, the UK ICO also undertook efforts to complete its regulatory framework post-Brexit. The most important development relates to the publication of draft international data transfer agreement ("**IDTA"**) and guidance, which were subject to consultation and are intended to replace the EU's legacy SCCs.[33]

B. Switzerland

As we indicated in the 2021 International Outlook and Review, on 25 September 2020, the Swiss Parliament adopted the revised version of the Federal Act on Data Protection 1992 ("**Revised FADP**"). In anticipation of its upcoming entry into law in the second half of 2022, on 5 March 2021, the Federal Data Protection and Information Commissioner ("**FDPIC**") published guidance on how the private sector and federal authorities needed to adapt their processing activities to comply with the new provisions of the Revised FADP. In particular, the guidance covers the right to data portability, codes of conduct, records of processing activities and cross-border transfers and extended requirements around providing information on data processing and transparency under the Revised FADP.[34]

On 23 June 2021, the Swiss Federal Council also released a draft revised Ordinance on the Federal Data Protection Act for public consultation following the adoption of the Revised FADP. In particular, the Council highlighted that the revisions to the Ordinance include minimum data security requirements, the modalities of the duty to inform data subjects, the right of access, data breach notification requirements, and exceptions to the obligation to keep a record of data processing activities for companies with fewer than 250 employees. Furthermore, the draft Ordinance specifies the criteria which the Council must take into account in its assessment of the adequacy of transfers of personal data to third countries, and includes a draft list of 34 countries which are considered to provide an adequate level of protection.[35]

With regard to data transfers, the FDPIC published a guide on 18 June 2021 to allow companies to review the admissibility of data transfers to third countries in accordance with the Federal Act on Data Protection 1992. The guide provides a flowchart detailing the actions required by organisations to ensure data transfers are made in compliance with the Act and, notably, elaborates on the legal requirement that apply to transfers to third countries that do not appear on the FDPIC list of adequate countries.[36]

Furthermore, on 27 August 2021, the FDPIC announced that the new SCCs adopted by the European Commission on 4 June 2021 for data transfers to third countries were also valid under Swiss law. The FDPIC recalled that the Commission's SCCs may be used by data exporters, provided that the necessary adaptations and amendments be made for use under Swiss data protection law (i.e., replacing references to the EU with references to Switzerland). In addition, in line with the timeline in the EU, the FDPIC confirmed that the European Commission's old SCCs could still be entered into until 27 September 2021 and existing agreements entered into under the old SCCs may still be used during a transitional period until 31 December 2022.[37]

C. Russia

As we indicated in the 2021 International Outlook and Review, Russia undertook a number of legislative modifications in 2021 to enhance and complete its data protection regime, notably in terms of increasing applicable fines.

In the same vein, Russia adopted a new federal law in 2021 'On Amendments to the Code of Administrative Offenses', which increased the amounts of administrative fines prescribed in the Code of Administrative Offenses against the Federal Law On Personal Data. The amendments do not touch upon the highest fines for breaching the data localisation requirement, but do increase the administrative fines for repeated offenses (i.e., offences that occur within one year from the date the previous violation was enforced). Recidivism concerning the localisation requirement may lead to fines between RUB 6,000,000 and 18,000, 000 (approximately USD 80,000 to 240,000) on companies, and responsible managers may face fines between RUB 500,000 and 800,000 (approximately USD 6,600 to 10,500).[38]

In addition, the Russian Federal Service for the Supervision of Communications, Information Technology and Mass Communications ("**Roskomnadzor**") and the Russian Parliament ("**Duma**") have continued to undertake efforts to protect Russian consumers and citizens. *First*, on 29 March 2021, the Ministry of Digital Development published draft amendments to the Federal Law of 27 July 2006 No. 152-FZ on Personal Data in order to require telecom operators to obtain the consent of subscribers prior to the sale of their personal data for telemarketing purposes.[39]

On 1 July 2021, the Roskomnadzor also announced that it had launched an online service allowing companies to obtain and record consent to the processing of personal data collected directly from the data subject. The Roskomnadzor claims that the template service will enable operators to meet the consent requirements following the entry into force of the amendments to the Federal Law on Personal Data in March 2021. Furthermore, the Roskomnadzor noted that the template may be customised to the specific activities of the operator, and that data subjects may record their preferences as to how their personal data may be processed and further distributed to third parties.

Finally, on 10 November 2021, the Duma registered a bill on 'Amendments to Article 14.8 of the Code of the Russian Federation on Administrative Offences' in order to prohibit companies from forcing consumers to provide personal data in cases where such data is not necessary to complete the transaction and is not provided for by legislation.[40]

D. Turkey

In 2021, the Turkish data protection authority ("**KVKK**") proceeded with its significant activity in providing guidance on the application of the Turkish Data Protection Act. Notably, on 20 October 2021, it issued guidance on the right to be forgotten ("**RTBF**") in respect of search engines. The guidance follows up on the KVKK Board Decision 2020/481 regarding the requests of individuals to remove names, surnames and the results of searches made through search engines from the index, and it aims to clarify issues relating to the exercise of the RTBF. Among other points, it indicates that the individuals may exercise the RTBF either by making a request to the data controller (search engine) or by complaining to the KVKK.[41]

Finally, throughout 2021, the KVKK continued with its enforcement of the Turkish Data Protection Act. For example, on 21 June 2021, it imposed a fine of TRY 800,000 (approx. €77,390) on an e-commerce site for data security and breach notification failures under the Turkish Data Protection Act. In particular, the KVKK noted that the investigation was triggered by a complaint that access to the information of

third-party companies was provided through the customer service panel on the e-commerce site.[42] On 3 September 2021, the KVKK published a summary of review of a decision concerning an online messaging service provider, in which it imposed a fine of TRY 1,950,000 (approx. €195,000) for allegedly failing to take necessary technical and administrative measures to ensure data security pursuant to the Act.[43]

III. Developments in Asia-Pacific

A. Australia

As explained in the 2021 International Outlook and Review, the Australian government is currently undertaking a wholesale review of the Privacy Act 1988 with a view to implementing significant reforms to the country's privacy regime. In October 2021, the Attorney-General's Department released a discussion paper considering the items raised in the issues paper published in October 2020 (and referred to in the 2021 International Outlook and Review) and has sought further feedback on the proposed reforms.[44] Submissions on the discussion paper closed on 10 January 2022, and those submissions will now form the basis of a final report to be submitted to government.

The discussion paper proposes wide-ranging reforms which would align Australia's privacy regime more closely to 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 or require its erasure and to modify the framework for international data transfers.

This review has been 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 on 25 October 2021.[45] The Online Privacy Bill proposes 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 and significantly broaden the extra-territorial reach of the Privacy Act 1988 to apply to acts performed outside Australia by foreign organisations carrying on business in Australia. Submissions on the Online Privacy Bill closed on 6 December 2021 and those submissions will inform further development of the Online Privacy Bill before its introduction to Parliament in 2022.

In addition to the ongoing review of the Privacy Act 1988 and the Online Privacy Bill, the US and Australian governments signed an agreement on 15 December 2021 to facilitate access to electronic data for investigations authorised by the Clarifying Lawful Overseas Use of Data (CLOUD) Act of 2018.[46] This agreement allows authorities from each country to access certain data directly from providers operating in the others' jurisdiction to mitigate, detect and investigate serious crimes, including ransomware attacks and terrorism, as well as crimes that sabotage critical infrastructure over the internet. The agreement will undergo parliamentary and congressional review procedures in 2022 and is intended to replace the mutual legal assistance mechanism currently used to access data from such providers, which relevant authorities perceive as too slow and awkward to fulfil its intended purpose.[47]

B. China

1. Passage of the Personal Information Protection Law

On 20 August 2021, the Standing Committee of China's National People's Congress passed the Personal Information Protection Law ("**PIPL**"), which took effect on 1 November 2021.[48] The PIPL applies to "personal information processing entities ('**PIPEs**')", defined as "an organisation or individual that independently determines the purposes and means for processing of personal information". The PIPL defines "personal information" broadly as "various types of electronic or otherwise recorded information relating to an identified or identifiable natural person", excluding anonymised information, and defines "processing" as "the collection, storage, use, refining, transmission, provision, public disclosure or deletion of personal information" (PIPL Article 4).

The PIPL shares many similarities with the EU's GDPR, including its extraterritorial reach, restrictions on data transfer, compliance obligations and sanctions for non-compliance, amongst others. The PIPL raises some concerns for companies that conduct business in China, even where such companies' data processing activities take place outside of China, and the consequences for failing to comply could potentially include monetary penalties and companies being placed on a government blacklist.

The PIPL applies to cross-border transmission of personal information and applies extraterritorially. Where PIPEs transmit personal information to entities outside China, they must inform the data subjects of the transfer, obtain their specific consent to the transfer and ensure that the data recipients satisfy standards of personal information protection similar to those in the PIPL. The PIPL applies to organisations operating in China, as well as to foreign organisations and individuals processing personal information outside China in any one of the following circumstances: (1) the organisation collects and processes personal data for the purpose of providing products or services to natural persons in China; (2) the data will be used in analysing and evaluating the behaviour of natural persons in China; or (3) under other unspecified "circumstances stipulated by laws and administrative regulations". This is an important similarity between the PIPL and GDPR, as the GDPR's data protection obligations apply to non-EU data controllers and processors that track, analyse and handle data from visitors within the EU. Similarly, under the PIPL, a foreign receiving party must comply with the PIPL's standard of personal information protection if it handles personal information from natural persons located in China.

The PIPL gives the Chinese government broad authority in processing personal information. State organisations may process personal information to fulfil statutory duties, but may not process the data in a way that exceeds the scope necessary to fulfil these statutory duties. Personal information processed by state organisations must be stored within China.

The PIPL establishes guiding principles on protection of personal information. According to the PIPL, processing of personal information should have a "clear and reasonable purpose" and should be directly related to that purpose. The PIPL requires that the collection of personal information be minimised and not excessive, and that PIPEs ensure the security of personal information. To that end, the PIPL imposes a number of compliance obligations on PIPEs, including requiring PIPEs to establish policies and

procedures on personal information protection, implement technological solutions to ensure data security and carry out risk assessments prior to engaging in certain processing activities.

The PIPL adopts a risk-based approach, imposing heightened compliance obligations in specified high-risk scenarios. For instance, PIPEs whose processing volume exceeds a yet-to-be-specified threshold must designate a personal information protection officer responsible for supervising the processing of personal data. PIPEs operating "internet platforms" that have a "very large" number of users must engage an external, independent entity to monitor compliance with personal information protection obligations, and regularly publish "social responsibility reports" on the status of their personal information protection efforts. The law mandates additional protections for "sensitive personal information", broadly defined as personal information that, once disclosed or used in an illegal manner, could infringe on the personal dignity of natural persons or harm persons or property. "Sensitive personal information" includes biometrics, religious information, special status, medical information, financial account, location information and personal information of minors under the age of 14. When processing "sensitive personal information", according to the PIPL, PIPEs must only use information necessary to achieve the specified purpose of the collection, adopt strict protective measures and obtain the data subjects' specific consent.

The PIPL creates legal rights for data subjects. According to the new law, PIPEs may process personal information only after obtaining fully informed consent in a voluntary and explicit statement, although the law does not provide additional details regarding the required format of this consent. The law also sets forth certain situations where obtaining consent is unnecessary, including where necessary to fulfil statutory duties and responsibilities or statutory obligations, or when handling personal information within a reasonable scope to implement news reporting, public opinion supervision and other such activities for the public interest. Where consent is required, PIPEs should obtain a new consent where it changes the purpose or method of personal information processing after the initial collection. The law also requires PIPEs to provide a convenient way for individuals to withdraw their consent, and mandates that PIPEs keep the personal information only for the shortest period of time necessary to achieve the original purpose of the collection. If PIPEs use computer algorithms to engage in "automated decision making" based on individuals' data, the PIPEs are required to be transparent and fair in the decision making, and are prohibited from using automated decision making to engaging in "unreasonably discriminatory" pricing practices. "Automated decision-making" is defined as the activity of using computer programs to automatically analyse or assess personal behaviours, habits, interests, hobbies, financial, health, credit or other status, and make decisions based thereupon. When individuals' rights are significantly impacted by PIPEs' automated decision making, individuals can demand PIPEs to explain the decision making and decline automated decision making.

The PIPL creates penalties for organisations that fail to fulfil their obligations to protect personal information. These penalties include disgorgement of profits and provisional suspension or termination of electronic applications used by PIPEs to conduct the unlawful collection or processing. Companies and individuals may be subject to a fine of not more than 1 million RMB (approximately $154,378.20) where they fail to remediate conduct found to be in violation of the PIPL, with responsible individuals subject to fines of 10,000 to 100,000 RMB (approximately $1,544 to $15,438). Companies and responsible individuals face particularly stringent penalties where the violations are "grave", a term left

undefined in the statute. In these cases, the PIPL allows for fines of up to 50 million RMB (approximately $7,719,027) or 5% of annual revenue, although the PIPL does not specify which parameter serves as the upper limit for the fines. Authorities may also suspend the offending business activities, stop all business activities entirely or cancel all administrative or business licenses. Individuals responsible for "grave" violations may be fined between 100,000 and 1 million RMB (approximately $15,438 to $154,383), and may also be prohibited from holding certain job titles, including Director, Supervisor, high-level Manager or Personal Information Protection Officer, for a period of time. In contrast, fines for severe violations of the GDPR can be up to €20 million (approximately $23,486,300) or up to 4% of the undertaking's total global turnover of the preceding fiscal year (whichever is higher).

For more details regarding potential issues for companies operating in China and the impact of the PIPL, please see our client alert here.

2. Draft Measures for Data Export Security Evaluations

On 29 October 2021, the Cyberspace Administration of China requested public comments on the draft Measures for Data Export Security Evaluation until 28 November 2021. The draft underscores the need to standardise data exports under the PIPL, Cybersecurity Law and Data Security Law. Under the draft, PIPEs transferring data which meets one of the following requirements outside of China are required to submit a report through the provincial Cyberspace Administration: (1) personal information and important data are generated by operators of critical information infrastructure; (2) outbound data contains important data; (3) personal information processors who have processed personal information of one million people; (4) personal information processors who have processed personal information of more than 100,000 people or sensitive personal information of more than 10,000 people abroad; or (5) other situations required by the Cyberspace Administration.

3. Regulations on the Security Protection of Critical Information Infrastructure

Following the United States' proposal of the Cyber Incident Notification Act of 2021 and the EU's adoption of Directive (EU) 2016/1148 on Security of Network and Information Systems in 2016, China introduced rules to protect the country from cyber-attacks on critical information systems. China's Regulations on the Security Protection of Critical Information Infrastructure (the "**Regulations**") took effect on 1 September 2021.[49]

The Regulations are a key feature of China's Cybersecurity Law, which was implemented on 1 June 2017. The Regulations protect the security of critical information infrastructure ("**CII**") and expand on the Cybersecurity Law by imposing additional compliance obligations. Article 31 of the Cybersecurity Law delegates further authority to the State Council to formulate specific security protection measures for CII. By enacting the Regulations, the State Council has broadened the definition of CII, clarified which authorities are responsible for CII protection, outlined the duties of CII operators and third parties in relation to testing / monitoring CII and established penalties for non-compliance.

The Cybersecurity Law defines CII as infrastructure from important industries, including public communication and information services, energy, transportation, water conservancy, finance, public services, e-government and other critical information infrastructure which may endanger national

security, national welfare, people's livelihoods or the public interest if data is disabled, damaged or leaked. The Regulations not only define CII as those industries identified in Article 31 of the Cybersecurity Law, but also national defence and technology industries. This includes:

- Public communications and information services;
- Energy;
- Transportation;
- Water conservancy;
- Finance;
- Public services;
- E-government;
- National defence science, technology and industry; and
- Other important network facilities and information systems that may severely threaten national security, national welfare, people's livelihood or the public interest if disabled, damaged or leaked.

The Regulations impose obligations on CII operators ("**CIIOs**"), including, but not limited to: (1) establishing a security management department; (2) conducting background checks on key personnel with the assistance of police and national security agencies; (3) conducting an annual risk audit and assessing security risks; (4) reporting cyber incidents or threats to relevant authorities (including the Cyberspace Administration and the State Council); (5) conducting cybersecurity reviews when the network products and services a CIIO purchases may influence national security; and (6) reporting any corporate activity that may impact cyber security, including mergers or dissolutions (Regulations Articles 15, 19, 21).

The Regulations prohibit any entity or individual from illegally invading, interfering with or destroying CII and carrying out loophole detection or permeability tests on CII (Regulations Article 5). Additionally, no entity or individual may carry out vulnerability monitoring, penetration testing or other such activities on CII that may influence or endanger the security of CII, unless such entity or individual has received approval from the national cyberspace and informatisation department, the State Council public security department or the relevant protection work department or operator (Regulations Article 31). If an entity or individual chooses to carry out such activities on basic telecommunications networks, it must report such activity in advance to the State Council department in charge of telecommunications (Regulations Article 31).

Under the Regulations, companies may face monetary fines of up to RMB 1 million (USD 155,000) for serious violations, and key individuals may face fines up to RMB 100,000 (US 15,000) (Regulations Articles 39, 40, 41, 42 and 43).

The Regulations will impact network operators as more network operators may be deemed CIIOs and more compliance obligations will likely be imposed by competent industry regulators. Network operators in critical industries should remain alert to their industry regulators and ensure their compliance programs align with the Regulations and the Cybersecurity Law. Global clients that operate in China in the identified industries and sectors should be aware of these requirements and alert to the prospect that they may be designed as CIIOs. Further, firms in the business of carrying out vulnerability monitoring or penetration testing on businesses in China operating in the industries outlined above should be conscious of the prospect that their clients could be considered CIIOs, and should ensure that they are seeking assurances from their clients that they are not CIIOs before undertaking this work. Alternatively, these firms should be prepared for the need to seek approval for this work from the national cyberspace and informatisation department, the State Council public security department or the relevant protection work department or operator.

4. Draft Regulations on Algorithmic Recommendation Technology

Chinese authorities announced the Internet Information Service Algorithmic Recommendation Management Provisions, which will come into force on 1 March 2022.[50] These regulations apply to technology such as personalised recommendations, search filters and any algorithms that provide content to users. These regulations cover various services, such as social media platforms and entertainment streaming. The regulations not only apply to the PIPL, but also the Cybersecurity Law, Data Security Law and the Internet Information Services Management Rules for the purpose of promoting national security and public interests.

C. India

As indicated in both the 2020 and 2021 International Outlook and Review, the Personal Data Protection Bill 2019 ("**PDP Bill**") was introduced in Indian Parliament on 11 December 2019 and subsequently referred to a Joint Parliamentary Committee ("**JPC**") for consideration. On 16 December 2021, after a prolonged review period, the JPC tabled its report and suggested amendments to the PDP Bill, which has not yet been enacted. The resulting report and amendments were primarily informed by the stated need to balance data-driven innovation while catering to national security demands. Some of the key recommendations include:[51]

- Expansion of the scope of the PDP Bill to cover both personal and non-personal data. The JPC suggested that consolidation of the regulatory framework in this manner was necessary in light of the impossibility to distinguish between personal and non-personal data when mass data is collected or transported.

- Preparation and implementation of data localisation policies to ensure that sensitive personal data or other critical data is stored and processed in India, and only transferred outside India with the DPA's approval (subject to government consultation).

- Establishment of a mechanism for the formal certification of digital and IoT devices to ensure their integrity with respect to data security.
- Assigning responsibility to social media platforms for the content hosted on their platforms and requiring those platforms to set up an office in India.
- Introduction of a fixed timeline of 72 hours for breach reporting.

The JPC recommended that a 24-month transitional period should apply for implementation of the PDP Bill to allow relevant parties to update their policies, infrastructure and processes. The JPC's report and amendments to the PDP Bill will be reviewed by the Parliament before being enacted. Until the PDP Bill is enacted, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 continue to govern data protection in India.

D. Indonesia

As identified in the 2021 International Outlook and Review, a draft of the Personal Data Protection Act ("**PDP Bill**") was submitted to the Indonesian House of Representatives on 24 January 2020.[52] The PDP Bill consolidates the rules related to personal data protection in Indonesia and is anticipated to establish data sovereignty and security as the keystone of Indonesia's data protection regime.[53]

On 1 September 2020, the Ministry of Communication and Information Technology of Indonesia ("**Kominfo**") issued a statement claiming that the PDP Bill would be completed by mid-November 2020.[54] However, as of the date of this review, the Indonesian House of Representatives is still yet to pass the PDP Bill due to ongoing debate over the position, form and independence of the authority slated to oversee its regulation and enforcement.[55] Despite this, the expectation is that the PDP Bill will be enacted in the first quarter of 2022.

E. Hong Kong

The Personal Data (Privacy) Ordinance ("**PDPO**"), passed in 1995, is one of Asia's longest standing data protection laws. The PDPO was amended in 2021 to combat doxxing acts which intrude on personal data privacy.

The Personal Data (Privacy) (Amendment) Bill 2021 ("**PDPO Bill**") came into effect on 8 October 2021 after the Hong Kong legislature passed the legislation on 29 September 2021.[56] The PDPO Bill criminalises doxxing acts, including imprisonment for five years and fines up to HK$1 million. In addition, the PDPO Bill empowers the Office of the Privacy Commissioner for Personal Data to persecute individuals for doxxing incidents and perform related criminal investigations.

F. Japan

1. APPI Amendments

As explained in the 2021 International Outlook and Review, the Parliament of Japan adopted a bill on 5 June 2020 to amend the currently applicable general data protection law, the Act on the Protection of Personal Information ("**APPI**"). The APPI will take force on 1 April 2022, while transitional measures for companies that share data with third parties took effect on 1 October 2021.

2. Review of EU-Japan Mutual Adequacy Agreement

On 26 October 2021, the Personal Information Protection Commission of Japan, the European Commission and other relevant authorities conducted the first review of the EU-Japan mutual adequacy arrangement effective in 2019. The Commissions will publish separate reports to conclude the review process.[57]

G. Mongolia

In 2021, the Standing Committees on Innovation and e-Policy and Legal Affairs in Mongolia opened discussions on a Draft Law on the Protection of Personal Information, which details data subject rights, requirements and responsibilities for data processors and controllers, and requirements for overseas data transfers.

H. New Zealand

The New Zealand Privacy Act 2020 ("**NZ Privacy Act**") came into force on 1 December 2020, repealing and replacing an existing 1993 act. 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. While the NZ Privacy Act remains less onerous than international equivalents, such as the GDPR, it nonetheless introduces significant reforms to the privacy regime in the country, such as mandatory data breach reporting, broader investigative and enforcement powers for the regulator and new criminal offences and penalties, including fines of up to NZ$10,000. Pursuant to the changes, the NZ Privacy Act applies extraterritorially to overseas organisations carrying on business in New Zealand and which hold information about New Zealand individuals.[58]

Despite these recent reforms, the Office of the Privacy Commissioner of New Zealand recommended in 2021 that "further changes are desirable" in response to fast-changing technologies. The proposed changes include the introduction of a right of personal information portability and a right to be forgotten, protection against the risk of re-identification from de-identified information, limitation of harm caused by automated decision making algorithms, increased civil penalties for non-compliance and expanded powers of the regulator to require compliance reporting by organisations subject to the NZ Privacy Act.[59]

I. 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**"). The proposed 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 extra-territorial 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 Commissioner of a data breach, widen the enforcement powers of the regulator and modify the criminal penalties for non-compliance.[60]

J. Singapore

As explained in the 2021 International Outlook and Review, data protection in Singapore is currently governed by the Personal Data Protection Act 2012 ("**Singapore PDPA**").

The initial phase of the Personal Data Protection (Amendment) Act 2020 (No. 40 of 2020) ("**Singapore PDPA Amendments**") took effect on 1 February 2021. On 1 February 2021, the Singapore PDPA Amendments' requirement for mandatory notification to the Personal Data Protection Commission ("**PDPC**") for data breaches came into force. This requires organisations to notify the PDPC no later than three calendar days after the organisation determines that a data breach is notifiable if either of the following occurs: (1) a data breach that results in or is likely to result in significant harm to the data subject or (2) a data breach of a significant scale (i.e. which involves more than 500 affected data subjects). The PDPC also made follow-up amendments on 1 October 2021 to clarify these situations.[61]

On 25 November 2021, the PDPC announced its collaboration with the Singapore Police Force and Cyber Security Agency of Singapore to develop a handbook on the Singapore PDPA, Cybersecurity Act 2018 (No. 9 of 2018) and Computer Misuse Act (Cap. 50A).[62]

On 9 December 2021, Singapore and the United Kingdom published a Digital Economy Agreement ("**DEA**"). The DEA aims to facilitate cross-border data flows while upholding data protection standards. Furthermore, both countries have committed that neither will introduce unjustified data localisation requirements, giving businesses in the United Kingdom a guarantee that they will not have to pay for data storage and processing in Singapore. The DEA will require both countries to maintain their data protection frameworks.[63]

K. South Korea

As explained in the 2021 International Outlook and Review, data protection in South Korea is currently governed by the Personal Information Protection Act ("**PIPA**").

As noted above, on 17 December 2021, the PIPC and the European Commissioner for Justice formally announced an adequacy agreement between South Korea and the European Union for transfers of personal data. This adequacy agreement promotes the transfer of personal data between South Korea and the European Union without additional mechanisms or authorisations for data transfers.[64]

L. 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.[65]

M. Thailand

As noted in both the 2020 and 2021 International Outlook and Review, the Personal Data Protection Act 2019 ("**Thailand PDPA**"), which is the first consolidated data protection law in Thailand, was originally expected to come into full effect on 27 May 2020. However, in May 2020, and then again in May 2021, the government of Thailand approved a Royal Decree to postpone the application of the Thailand PDPA until 31 May 2021 and, subsequently, 31 May 2022, citing the negative effects of the COVID-19 pandemic and the requirement for further legislative work as the primary reasons for doing so.[66]

Reference must be made to the fact that the Thailand PDPA is largely modelled upon the GDPR, containing many similar provisions, although they differ in areas such as anonymisation. Moreover, the Thailand PDPA provides for the creation of a 16-member Personal Data Protection Committee ("**PDPC**"), which is yet to be fully established. As such, the MDES is currently acting as the supervisory authority for any data protection–related issues within Thailand. Once created, the PDPC is expected to adopt notices and regulations to clarify and guide data controllers and other stakeholders on how to prepare for and remain compliant with the requirements under the Thailand PDPA once it is passed.

N. Vietnam

As explained in the 2021 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, which sets out principles of data protection, including purpose limitation, data security, data subject rights and the regulation of cross-border data transfers. Moreover, the Draft PDPD contains 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 remains unissued, with little clarity over the timing of the parliamentary process required for it to come into effect.

IV. Developments in Africa

A. Botswana

On 15 October 2021, the **Data Protection Act** entered into effect, more than three years after it was passed by the National Assembly on 12 July 2018. The Act's transition period is 12 months from the date of commencement and will automatically end on 15 October 2022, meaning that data controllers,

including companies and organisations, must take compliance measures until that date. The Act requires data controllers and processors to respect in their processing: the lawfulness and fairness of processing, imposes limitations with respect to the purpose of processing, personal data retention and minimisation, in addition to other protections concerning the relevance and adequacy, integrity and confidentiality of personal data collected by entities. Further, the Act provides for data subject rights, including the right to be informed, the right to access, the right to be given reasons if the access is denied, the right to object and revoke consent and the right to raise a challenge for purposes of deletion and amendment, in addition to setting out restrictions of matters such as direct marketing, sensitive data and data transfers. The Act creates the Information and Data Protection Commission, which will be responsible to protect the personal rights of individuals with regard to their personal data, and to ensure the effective application and enforcement of the Act. Unlike the GDPR, the Act also provides for significant potential prison terms ranging from three to 12 years for certain violations.[67]

B. Kenya

In 2021, the Ministry of ICT, Innovation and Youth Affairs launched a public consultation on three draft data protection regulations, which remained open until 11 May 2021:

- The **Data Protection (General) Regulations 2021**, which set out the procedures for enforcement of the rights of the data subjects and outline the duties and obligations of the data controllers and data processors.

- The **Data Protection (Registration of Data Controllers and Data Processors) Regulations 2021**, which define the procedure that will be adopted by the Office of the Data Commissioner in registering data controllers and data processors.

- The **Data Protection (Compliance and Enforcement) Regulations, 2021**, which outline the compliance and enforcement provisions for Data Commissioner, Data Controllers and Data Processors.

In January 2021, the Office of the Data Protection Commissioner published a guidance note on access to personal data during the Coronavirus pandemic. According to the guidance, the access and processing of personal data of individuals in response to the pandemic is subject to the Data Protection Act No. 24 of 2019. The key principles emphasised by the guidance include the processing of personal data in an accountable manner, the maintenance of the integrity and confidentiality of data and the responsibility for the implementation of a protection and safeguarding personal data mechanism.[68]

C. Nigeria

The National Information Technology Development Agency ("**NITDA**") announced in a press release on 12 November 2021 its collaboration with the Federal Competition and Consumer Protection Commission ("**FCCPC**") in order to combat data privacy abuse by money lending operators.[69] The partnership is anticipated to provide a more robust and concerted regulatory approach while ensuring that Nigerians get necessary reprieve from the illegal use of their personal data for money lending

operations, including through joint investigations, enforcement and possible prosecution for non-compliance.[70]

In this regard, NITDA announced, on 17 August 2021, that it had fined Soko Loans Lending Company Limited NGN 10 million (approx. €20,700) for various violations of the **Nigeria Data Protection Regulation, 2019** ("**NDPR**"), marking the first fine issued under the NDPR. NITDA outlined that the fine followed an investigation into a series of complaints against Soko Loans for unauthorised disclosures, failure to protect customers' personal data and defamation of character, as well as failure to carry out the necessary due diligence required by the NDPR. Soko Loans grants its customers uncollateralised loans and requires them to download its mobile application on their phone and activate a direct debit in the company's favour. The app gains access to the borrowing customer's phone contacts. Following the complainant customers' failures to meet loan repayment obligations, the company unilaterally sent privacy invading messages to their contacts (who were neither were parties to the loan transaction nor consented to the processing of their data). In addition, NITDA found that Soko Loans embedded trackers that share data with third parties inside its mobile application without providing users information about it or using the appropriate lawful basis. NITDA therefore found that Soko Loan and its entities violated multiple provisions of the NDPR.

In addition to a financial penalty, NITDA compelled Soko Loans to suspend the issuance of privacy-invading messages to any Nigerian until the company and its entities show full compliance with the NDPR, paid for the conduct of a Data Protection Impact Assessment by a NITDA appointed DPCO, and were placed on mandatory Information Technology and Data Protection supervision for nine months.[71]

D. Rwanda

Law No. 058/2021 of 13 October 2021 Relating to the **Protection of Personal Data and Privacy** (the "**Law**") came into effect upon its publication in the Rwanda Official Gazette on 15 October 2021. The Law establishes provisions relating to the processing of personal data, including the rights of the data subject such as the right to object to the processing of personal data, to personal data portability, to the erasure of personal data and to rectification of incorrect personal information.

The Law also provides for the duties and powers of the supervisory authority relating to the protection of personal data and privacy, stipulates the obligations and registration requirements of data controllers and processors, and includes provisions regarding the sharing, transfer and retention of personal data. Moreover, the Law provides for the consequences and sanctions of non-compliance, including fines ranging from RWF 2,000,000 (approx. €1,500) to RWF 5,000,000 (approx. €4,243) or, in the case of a corporate body or legal entity, 1% of their global turnover in the preceding financial year.

The Law provides for a two-year transitional period before its application to data controllers or data processors who are already in operation.[72] The **National Cyber Security Authority** ("**NCSA**") has been designated as the supervisory authority in charge of enforcement of the Law.[73]

On 10 December 2021, the NCSA issued a notice on the Personal Data Law detailing that the Personal Data Law requires all those who wish to process personal data to register with the NCSA as a data controller or data processor.[74]

On 14 December 2021, the NCSA also published a notice clarifying that consent of the data subject is a key foundation to the lawful collection and processing of personal data and may be made in oral, written or electronic format.[75]

E. South Africa

The enforcement powers of the supervisory authority of South Africa (the "**Information Regulator**") under the **Protection of Personal Information Act, 2013** ("**POPIA**") came into effect on 1 July 2021, following the conclusion of a 12-month transitional grace period.[76]

In 2021, the Information Regulator issued a set of notices and rules for guidance on different sections of POPIA. Notably:

- Guidance note on the processing of special personal information under sections 26 and 27(1) of POPIA to guide responsible parties who are required to obtain authorisation from the Information Regulator to process special personal information, as provided for in section 27(2) of POPIA. The guidance provides for the manner of submission of an application for authorisation and outlines specific exemptions in which the prohibition on processing of personal information does not apply.[77]

- Guidance note on Exemptions from the Conditions for Lawful Processing of Personal Information under sections 37 and 38 of POPIA. In particular, the guidance outlines that these exemptions include that the processing is either in the public interest or involves a clear benefit to the data subject.[78]

- Rules on the manner in which a complaint must be submitted and handled by the Information Regulator which will come into operation on a future date that the Information Regulator determines.[79]

On the enforcement front, the Information Regulator has initiated its action by targeting both local and international businesses. For example, in a media statement published on 13 May 2021, the Information Regulator announced that it was preparing a litigation opinion contending the need for an online messaging service provider to adopt its EU privacy policy in South Africa and other developing countries with frameworks similar to the GDPR. However, the service provider has so far declined to make any revisions to its South African privacy policy.[80]

Finally, on 1 June 2021, the President assented to the **Cybercrimes Act 19, 2020**, which intends to criminalise the disclosure of harmful data messages, regulate relevant government authorities' powers to investigate cybercrimes, provide for the establishment of a designated Point of Contact and impose obligations to report cybercrimes. The President has not yet proclaimed the commencement date of this new legislation.[81]

F. Other African Jurisdictions

Other developments in 2021 in data protection and cybersecurity regulation in Africa include:

- **Togo**: On 29 June 2021, the National Assembly adopted a Bill authorising the ratification of the **Convention on Cyber Security and Personal Data Protection**. According to the National Assembly, this convention will strengthen the country's legal framework for electronic transactions, the protection of personal data and the fight against cybercrime.[82]

- **Uganda**: The **Data Protection and Privacy Regulations, 2021** of the Republic of Uganda ("the **Regulations**") came into force on 12 March 2021. The Regulations establish provisions for the collection and processing of personal data and the rights of data subjects in regard to their personal data, in addition to establishing an independent **Personal Data Protection Office** ("**PDPO**") in the National Information Technology Authority of Uganda ("**NITA-U**"), which shall be responsible for personal data protection and privacy and for the implementation of the Data Protection and Privacy Act, 2019, including the imposition of administrative, civil or criminal sanctions for non-compliance. [83]

On 2 November 2021, the PDPO issued a press release announcing that it required data collectors, processors and controllers to register on its website before the end of the grace period of 31 December 2021 and that it will begin enforcement measures for those that do not in January 2022.[84]

- **Zambia**: On 23 March 2021, the Parliament of Zambia enacted the **Data Protection Act No. 3 of 2021**, which stipulates a system for the use and protection of personal data by regulating the collection, use, transmission, storage and processing of personal data. The Act also establishes the Office of the Data Protection Commissioner and outlines the duties of data controllers and data processors, the rights of data subjects and the conditions for cross-border transfer of personal data. The Minister will appoint the date of the commencement of the Act by statutory instrument.[85]

- **Zimbabwe**: The **Data Protection Act [Chapter 11:12]** was enacted on 3 December 2021. The Act provides for the establishment of the Cyber Security and Monitoring Center and the designation of the Postal and Telecommunications Regulatory Authority of Zimbabwe ("**POTRAZ**") as the data protection authority. The Act addresses the processing of personal data collected and processed by companies, cross-border transfers of personal data, and general provisions, including the appeals process, offences and penalties. The Act does not establish a date of application or a transitional period prior to its application.[86]

V. Developments in the Middle East

A. Israel

On 6 January 2022, the Government of Israel published a Bill[87] amending and updating Israel's Protection of Privacy Law, 5741-1981 ("**PPL**").[88] The Deputy Prime Minister and the Minister of Justice announced that the Bill aims to protect citizens and adapt the PPL's provisions and enforcement

to the current digital era. The most noteworthy amendments, summarised by Israel's Privacy Protection Authority ("**PPA**"), include the expansion of PPA's substantive investigation and enforcement powers, including the imposition of administrative sanctions in an amount up to 3.2 million NIS ($1 million), the adaptation of definitions in the law to technological and social developments, and the reduction of bureaucratic burdens through a significant reduction in the obligation to register databases.[89] The Bill would be effective six months after its approval by the parliament.

Before the introduction of the Bill, a ransomware attack on sensitive data of more than 290,000 Israeli medical patients and members of an LGBTQ+ website was reported. An Iranian-based hacking group targeted host program CyberServe and, on 2 November 2021, released the data, demanding a ransom of $1 million that the company refused. Israel's National Cyber Directorate had previously warned CyberServe on multiple occasions that its systems were not secure.[90] The ransomware attack was followed by a press release of the U.S. Department of the Treasury on 14 November 2021, announcing that it established a partnership with Israel to combat ransomware.[91]

On the enforcement side, on 23 May 2021, the PPA announced that, following a serious information security incident that resulted in the disclosure of sensitive personal information from the databases of the Hod Hasharon Municipality, it had determined that the Hod Hasharon Municipality had violated the Privacy Protection Law and regulations under it. The PPA's investigation concluded that sensitive personal information, including documents, email correspondence and complaints from residents (including names and ID numbers and information about employees using municipal systems) contained in the municipality's database, was accessible to unauthorised persons, and that the municipality did not take appropriate measures to assure that access to the database was carried out by authorised users. Additionally, according to the PPA's findings, the municipality had not conducted an assessment to identify security risks in its systems at the required time and did not correct the findings of a previous assessment, as required by the Protection of Privacy (Data Security) Regulations, 5777 - 2017. In light of this, the PPA gave the municipality instructions to correct the deficiencies discovered and fined it NIS 10,000 (approx. €2,530) for failing to register databases required to be registered under the provisions of the PPL.[92]

In his efforts to support the global fight against COVID-19, Israel's Prime Minister Benjamin Netanyahu announced an agreement between the Israeli Ministry of Health ("MoH") and Pfizer for an expedited supply of COVID-19 vaccines to Israel, under which Israel agreed to share with Pfizer "statistical data that would help develop strategies for defeating the coronavirus". In order to address privacy and transparency concerns, the MoH published a partially redacted version of its Real-World Epidemiological Evidence Collaboration Agreement with Pfizer. The agreement provides that the MoH will share "aggregate de-identified data" and jointly analyse such data with Pfizer. In particular, the MoH is required to provide "data transfers" that include, "at a minimum", weekly counts of confirmed COVID-19 cases, hospitalisations, severe or critical cases, ventilator use, deaths, symptomatic cases, vaccines given "by age and other demographic subgroups" and COVID-19 cases by age groups "and other demographic factors". The MoH undertook to provide such data "solely in a form rendered anonymised by the MoH in accordance with Regulatory Requirements" so that the data could not reasonably be used to re-identify the identity of an individual.[93]

B. United Arab Emirates

In late 2021, the UAE issued its first federal data protection law (Federal Decree Law No. 45/2021 on the Protection of Personal Data) (the "**Data Protection Law**"), alongside a law establishing the new UAE Data Office with the mandate to ensure the full protection of personal data, monitor the application of the Data Protection Law and issue necessary guidelines and instructions for its implementation (Federal Decree Law No. 44/2021 on Establishing the UAE Data Office).

According to the announcement of the Cabinet of UAE,[94] the Data Protection Law relevantly:

- has extraterritorial effect and applies to the processing of personal data (a) inside the country or (b) outside the country about data subjects within the country;
- prohibits the processing of personal data without the consent of its owner (subject to prescribed exceptions);
- defines the controls for the processing of personal data and the general obligations of companies that have personal data to secure personal data and maintain its confidentiality;
- defines the rights and cases in which the owner has the right to request correction of inaccurate personal data, restrict or stop the processing of personal data; and
- sets out the requirements for the cross-border transfer and sharing of personal data for processing purposes.

The Data Protection Law became effective on 2 January 2022. Executive regulations are due to be issued within six months of the date of issuance of the Data Protection Law (i.e. by 20 March 2022). UAE companies will then have six months from the issuance of those executive regulations to comply with the Data Protection Law (although that period may be extended by the Cabinet).[95]

On 14 February 2021, following public consultation conducted in 2020, the Abu Dhabi Global Market ("**ADGM**") announced that it had enacted the Data Protection Regulations 2021, which replaced the Data Protection Regulations 2015. In its announcement, ADGM endorsed the EU's GDPR for its robust data protection provisions and outlined that the new Regulations intend to be proportionate and business friendly, without undermining the key ambition of achieving a high standard of protection for personal data. Acknowledging that the adoption of the new Regulations will result in additional responsibilities for data controllers and data processors, ADGM proposed a transitional grace period of 12 months for current establishments and six months for new establishments, starting from 14 February 2021.[96] The Office of Data Protection ("**ODP**") has been established to monitor the compliance with the new Regulations.[97] The ODP has also published several guidance notes and templates to support ADGM entities and authorities in compliance with the Regulations.[98]

C. Other Middle East Jurisdictions

Other developments in 2021 in data protection and cybersecurity regulation in the Middle East include:

- **Jordan**: On 29 December 2021, the Council of Ministers approved a draft law on the protection of personal data.[99] The draft law intends to protect personal data in light of the ease of its collection, retention and processing, and to prevent attacks on the rights of citizens. The law also aims to establish a safe and stable online environment and define the obligations of persons responsible for personal data. A personal data protection board will be established to enforce the draft law. The draft law became publicly available in January 2022[100] and its commencement will follow upon approval by the parliament and the king.

- **Pakistan**: On 25 August 2021, the Ministry of Information Technology ("**MOITT**") published a revised draft for consultation on the Personal Data Protection Bill 2021. The revised draft provides for the establishment of the National Commission for Personal Data Protection. The draft includes also provisions for the cross-border transfer of personal data, the right to data portability and the right not to be subject to a decision based solely on automated processing. Unlike the previous draft Personal Data Protection Bill 2020, which was presented to the Cabinet of Pakistan for approval in April 2020, the revised draft requires data controllers to notify the supervisory authority and the data subject in the event of a data breach without undue delay and, where reasonably possible, not beyond 72 hours of becoming aware of the breach.[101]

- **Qatar**: On 16 August 2021, the Qatar Financial Centre ("**QFC**") Authority launched a public Consultation Paper proposing changes to the QFC Data Protection Regulations and Rules.[102] The proposed changes aim to make the scope of the QFC Data Protection Regulations consistent with the provisions of international data protection laws and reflect the needs for expanded digitalisation in a global business environment. The amendments, inter alia, propose additional rights for data subjects and increased responsibilities for data controllers and data processors. On 31 January 2021, the Compliance and Data Protection Department at the Ministry of Transport and Communications released guidelines on the Personal Data Privacy Protection Law No. 13 of 2016 to inform individuals, regulated entities and stakeholders on their respective responsibilities, rights and practices as per the amended law.[103]

- **Saudi Arabia**: The National Centre for Documents and Archives Royal Court published, on 24 September 2021, the new Personal Data Protection Law ("**PDPL**"), marking the introduction of Saudi Arabia's first data protection law. The PDPL includes provisions for data controllers, the rights of data subjects and sanctions for non-compliance. The PDPL will come into force 180 days after the date of its publication in the Official Gazette.[104] In the field of cybersecurity, the Regulatory Framework for Cyber Security for Service Providers in the Communications, Information Technology and Postal Sector came into force on 29 May 2021. That framework intends to raise the level of cybersecurity maturity of service providers by requiring them to improve their cybersecurity risk management in accordance with international best practices and frameworks.[105]

VI. Developments in Latin America and the Caribbean

A. Brazil

As we indicated in the 2021 International Outlook and Review, the biggest data protection development in Brazil in 2020 was the entry into force of Law No. 13.709 of 14 August 2018 and the General Personal Data Protection Law (as amended by Law No. 13.853 of 8 July 2019) ("**LGPD**"), on 18 September 2020.

During 2021, the Brazilian data protection authority ("**ANPD**") adopted and published a series of guidance and FAQs regarding the LGPD. In particular:

- Guidance for Personal Data Processing Agents and Data Protection Officers, which aims to resolve common issues, set out non-binding guidelines for data processing agents and explain who may exercise the role of a data controller, operator and/or data protection officer. For each of those roles, the Guidance also specifies their respective liability regime, legal definition and example cases, in addition to FAQs regarding the same.[106]

- FAQs related to the commencement of the application of sanctions and fines under the LGPD.[107]

- Regulation CD/ANPD No. 1, on the Inspection Process and the Sanctioning Administrative Process', which aims to establish procedures with respect to the conduct of inspections and rules with respect to the administrative processes carried out by the ANPD. Moreover, the Regulation covers topics such as inspection, monitoring, guidance, injunctive measures and provides for an administrative fining procedure.[108]

- FAQs on data subjects' rights to petition controllers to enforce their data subject rights under the LGPD, which provide guidance on, among other things, procedures to be observed by data controllers, as well as the right of data subjects to complain about possible irregularities regarding the processing of their personal data.[109]

Finally, while the ANPD assumed its enforcement and fining powers, other Brazilian authorities have applied and enforced rules that concerned the protection of personal data in their territories. For example, on 14 June 2021, the Brazilian Federal Department of Consumer Protection of the National Consumer Secretariat ("**SENACON**") announced that it had fined Banco Cetelem S.A. with BRL 4,000,000 (approx. €653,200) for financial fraud that included the contracting of payroll loans with the improper use of personal data of elderly consumers.[110] In addition, on 13 July 2021, the Protection and Consumer Defence Foundation of the State of Mato Grosso ("**Procon-MT**") fined the pharmacies Droga Raia S.A and Drogasil S.A BRL 572,680.71 (approx. €94,210) for the irregular receipt of authorisation from customers for the processing and use of their data.[111]

B. Developments in Other Latin American and Caribbean Jurisdictions

There have also been significant developments in the adoption and enforcement of cybersecurity and data privacy laws in other Central and South American jurisdictions in 2021. We have set out highlights in key countries below:

- **Argentina**: On 16 April 2021, the Central Bank of Argentina ("**BCRA**") published guidelines on cybersecurity incident response and recovery. The BCRA noted that the guidelines are aimed at financial institutions, payment service providers that offer payment accounts and financial market infrastructures. However, the BCRA highlighted that, due to their general nature, the guidelines can also be adopted by any institution in the financial sector, as well as by information technology and communication service providers, among others.[112]

- **Chile**: On 5 November 2021, the Information Security Incident Response Team ("**CSIRT**") released cybersecurity guidelines for small and medium-sized enterprises ("**SMEs**"). In particular, the guidelines aim at supporting SMEs in the digitalisation process in a secure manner, helping them manage risks of data breaches, loss of business continuity, phishing, ransomware and other cyber threats.[113]

- **Costa Rica**: On 12 February 2021, the Bill No. 22.388 was published to Reform the Law on the Protection of Persons Regarding the Processing of their Personal Data No. 8968 of 2011. In particular, the bill aims to reform the current data protection law in Costa Rica by, among other things, improving the legal definitions for certain technical concepts (e.g., biometric data, genetic data and pseudonymisation), developing the principles governing the processing of personal data (such as transparency and data minimisation), improving data subject rights; strengthening the Costa Rican data protection authority, and strengthening the sanctions regime.

- **Ecuador**: On 21 May 2021, the Organic Law on the Protection of Personal Data was published, triggering a two-year grace period for companies and other entities that process personal data to adapt their operations to the new law.[114]

- **Panama**: On 28 May 2021, the National Authority of Transparency and Access to Information ("**ANTAI**") announced that the President of the Republic of Panama approved the Executive Decree No. 285 of 28 May 2021 that regulates the Law No. 81 on Personal Data Protection. The Executive Decree obliges all companies to put in place protocols or procedures to process data in compliance with the new law. Furthermore, the Executive Decree includes general provisions, information gathering requirements, the functions of the new role of data protection officer and the criteria for applying sanctions.[115]

- **Paraguay**: On 30 April 2021, the Chamber of Deputies announced the official presentation of the bill on the Protection of Personal Data of the Republic of Paraguay. The bill provides for the regulation of, among other things, data subject rights, security standards and obligations, data protection officer activities, and issues related to the creation of and procedures applicable to a supervisory authority.[116]

- **Uruguay**: On 16 September 2021, the Uruguayan data protection authority ("**URCDP**") announced the adoption of Resolution No. 23/021 of 8 June 2021, which implements important changes in the international data transfer regime in Uruguay. In particular, the resolution excludes the U.S. from the list of territories considered appropriate, in addition to suggesting the use of other mechanisms to transfer personal data abroad (e.g., contractual clauses, consent of the

interested parties and other elements justifying transfers). Moreover, to assist data controllers and processors, the URCDP published Resolution No. 41/021 of 8 September 2021, which includes a guide for the drafting of contractual clauses to transfer personal data.[117]

VII. Conclusion

As can be seen, 2021 was an eventful year in the field of data protection and privacy worldwide. In addition to the recently adopted laws and regulations on data privacy adopted by China, UAE, Brazil and Mexico, international lawmakers put a special focus on the regulatory treatment of key issues such as data localisation and transfers (e.g., in the EU, Russia and India).

2022 promises to be an equally active year from a legal and enforcement perspective, as regulators worldwide commence to make use of new legal tools and apply their respective national laws. We will continue to monitor the events in this space, and cover them in our monthly updates and in the Outlook and Review of 2023.

---

[1] *See* http://curia.europa.eu/juris/document/document.jsf;jsessionid=2BDC80771D0FB7EA8B6F60B9A3C4F572?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=20032710.

[2] *See* https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf.

[3] *See* https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf.

[4] *See* https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

[5] *See* https://edpb.europa.eu/system/files/2021-07/edpb_guidelinescodesconducttransfers_publicconsultation_en.pdf.

[6] *See* https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-052021-interplay-between-application_en.

[7] *See*, e.g., the French CNIL published guidance on the implementation of the SCCs, two Q&As on the content and the consequences of the *Schrems II* ruling, as well as a methodology to help controllers identify and process data transfers outside of the EU. German authorities released revised recommendations and updated guidance on international data transfers. The UK ICO launched a public

consultation on its draft international data transfer agreement that would replace the current SCCs to take into account the *Schrems II* ruling.

[8] *See* https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9703988.

[9] *See* http://www.raadvst-consetat.be/Arresten/251000/300/251378.pdf#xml=http://www.raadvst-consetat.be/apps/dtsearch/getpdf.asp?DocId=42765&Index=c%3a%5csoftware%5cdtsearch%5cindex%5carrets%5fnl%5c&HitCount=10&hits=28+29+2c+6b+de+17a+1de+505+150c+1884+&111112020 21318.

[10] *See* https://edpb.europa.eu/news/national-news/2021/bavarian-dpa-baylda-calls-german-company-cease-use-mailchimp-tool_en.

[11] *See* https://edpb.europa.eu/news/national-news/2021/census-2021-portuguese-dpa-cnpd-suspended-data-flows-usa_en.

[12] *See* https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2021-03-12/450163.

[13] *See* https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3183.

[14] *See* https://ec.europa.eu/info/sites/default/files/1_1_180366_dec_ade_kor_new_en.pdf.

[15] Relatedly, some Member States have continued to update their e-privacy legislation under the e-Privacy Directive. For example, in Germany, the Data Protection and Privacy in Telecommunications and Telemedia Act was enacted effective 1 December 2021, and contains comprehensive data protection regulations in the e-privacy field.

[16] *See* https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333.

[17] *See* https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202006_psd2_afterpublicconsultation_en.pdf.

[18] *See* https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf.

[19] *See* https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf.

[20] *See* https://edpb.europa.eu/system/files/2021-10/edpb_guidelines202010_on_art23_adopted_after_consultation_en.pdf.

[21] *See* https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012021_pdbnotification_adopted_en.pdf.

[22] *See* https://edpb.europa.eu/sites/default/files/files/file1/edpb_strategy2021-2023_en.pdf.

[23] *See* https://edpb.europa.eu/system/files/2021-03/edpb_workprogramme_2021-2022_en.pdf.

[24] *See* https://curia.europa.eu/juris/document/document.jsf?text=&docid=242821&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=558920.

[25] *See* https://d18rn0p25nwr6d.cloudfront.net/CIK-0001018724/cbae1abf-eddb-4451-9186-6753b02cc4eb.pdf.

[26] *See* https://justice.public.lu/fr/actualites/2021/12/communique-presid-trib-adm-ordonnance-amazon-cnpd.html.

[27] *See* https://www.cnil.fr/en/cookies-cnil-fines-google-total-150-million-euros-and-facebook-60-million-euros-non-compliance.

[28] *See*, e.g. Lower-Saxony Supervisory Authority https://lfd.niedersachsen.de/startseite/infothek/presseinformationen/lfd-niedersachsen-verhangt-bussgeld-uber-10-4-millionen-euro-gegen-notebooksbilliger-de-196019.html.

[29] *See*, e.g. Spanish AEPD https://www.aepd.es/es/documento/ps-00059-2020.pdf and Italian Garante https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9570980.

[30] *See*, e.g. Norwegian Datatilsynet https://www.datatilsynet.no/en/regulations-and-tools/regulations/avgjorelser-fra-datatilsynet/2021/gebyr-til-grindr/ and Spanish AEPD https://edpb.europa.eu/news/national-news/2021/spanish-data-protection-authority-aepd-imposes-fine-6000000-eur-caixabank_en.

[31] *See* https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/11/ico-issues-provisional-view-to-fine-clearview-ai-inc-over-17-million/.

[32] *See* https://ico.org.uk/action-weve-taken/enforcement/.

[33] *See* https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/08/ico-consults-on-data-transferred-outside-of-the-uk/.

[34] *See* https://www.edoeb.admin.ch/dam/edoeb/en/dokumente/2021/revdsg.pdf.download.pdf/revDSG_EN.pdf.

[35] *See* https://www.bj.admin.ch/dam/bj/fr/data/staat/gesetzgebung/datenschutzstaerkung/vdsg/vorentw.pdf.

[36] *See* https://www.edoeb.admin.ch/dam/edoeb/en/dokumente/2021/Anleitung für die Prüfung von Datenübermittlungen mit Auslandbezug EN.pdf.download.pdf/Anleitung für die Prüfung von Datenübermittlungen mit Auslandbezug EN.pdf.

[37]&nbnbsp; *See* https://www.edoeb.admin.ch/edoeb/en/home/latest-news/aktuell_news.html#-1259254222.

[38] *See* https://iapp.org/news/a/level-up-russia-enhances-the-protection-of-personal-data/#:~:text=Russia%20amends%20data%20protection%20law%20to%20increase%20personal%20data%20subjects'%20rights,-schedule%20May%2013&text=Beginning%20March%2027%2C%202021%2C%20Russia,period%20for%20data%2Drelated%20breaches.

[39] *See* https://rg.ru/2021/03/29/sotovym-operatoram-zapretiat-tajno-prodavat-dannye-klientov.html.

[40] *See* https://sozd.duma.gov.ru/bill/1184517-7#bh_note.

[41] *See* https://kvkk.gov.tr/SharedFolderServer/CMSFiles/11b6fd99-d42a-45b1-a009-21f2d36ded21.pdf.

[42] *See* https://kvkk.gov.tr/Icerik/6981/2021-427.

[43] https://www.kvkk.gov.tr/Icerik/7045/WHATSAPP-UYGULAMASI-HAKKINDA-YURUTULEN-RESEN-INCELEMEYE-ILISKIN-KAMUOYU-DUYURUSU.

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

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

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

[47] *See* https://www.itnews.com.au/news/australia-and-us-sign-cloud-act-deal-for-cross-border-data-access-574128.

[48] An unofficial English translation of the newly enacted PIPL is available at <https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-effective-nov-1-2021> and the Mandarin version of the PIPL is available at <http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml>.

[49] An unofficial translation of the Regulations is available <https://digichina.stanford.edu/news/translation-critical-information-infrastructure-security-protection-regulations-effective-sept>.

[50] An unofficial English translation of the Internet Information Service Algorithmic Recommendation Management Provisions is available at <https://digichina.stanford.edu/work/translation-internet-information-service-algorithmic-recommendation-management-provisions-effective-march-1-2022/>.

[51] See https://www.dsci.in/sites/default/files/Summary-%20and-Primer-on-Joint-Parliamentary-Committee-Report-and-Data-Protection-Bill-2021.pdf.

[52] Press release (in Indonesian) available athttps://www.kominfo.go.id/content/detail/24039/siaran-pers-no-15hmkominfo012020-tentang-presiden-serahkan-naskah-ruu-pdp-ke-dpr-ri/0/siaran_pers; the PDP Bill (in Indonesian) is available athttps://web.kominfo.go.id/sites/default/files/users/4752/Rancangan%20UU%20PDP%20Final%20%28Setneg%20061219%29.pdf.

[53] Press release (in Indonesian) available athttps://www.kominfo.go.id/content/detail/24041/menkominfo-indonesia-akan-menjadi-negara-ke-5-di-asean-pemilik-uu-pdp/0/berita_satker.

[54] Press release (in Indonesian) available athttps://www.kominfo.go.id/content/detail/29084/siaran-pers-no-104hmkominfo092020-tentang-pemerintah-apresiasi-pandangan-fraksi-terhadap-ruu-pdp/0/siaran_pers.

[55] *See* https://kr-asia.com/indonesia-needs-a-data-protection-authority-but-cant-decide-how-to-create-one.

[56] The PDPO Bill is available at <https://www.gld.gov.hk/egazette/pdf/20212540/es12021254032.pdf>.

[57] For more information on the first review of the EU-Japan mutual adequacy arrangement, please click <https://ec.europa.eu/newsroom/just/items/724795/en>.

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

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

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

[61] The PDPC's updated advisory guidelines are available at https://www.pdpc.gov.sg/Guidelines-and-Consultation/2020/03/Advisory-Guidelines-on-Key-Concepts-in-the-Personal-Data-Protection-Act and <https://www.pdpc.gov.sg/Guidelines-and-Consultation/2020/02/Advisory-Guidelines-on-the-Personal-Data-Protection-Act-for-Selected-Topics>.

[62] The handbook on the Singapore PDPA, Cybersecurity Act 2018 (No. 9 of 2018), and Computer Misuse Act (Cap. 50A) is available at <https://www.csa.gov.sg/News/Publications/overview-of-legislations>.

[63] More information on the Digital Economy Agreement between Singapore and the United Kingdom is available at <https://www.gov.uk/government/publications/uk-singapore-digital-economy-agreement-agreement-in-principle-explainer/uk-singapore-digital-economy-agreement-agreement-in-principle-explainer>.

[64] The adequacy decision between South Korea and the European Union is available at <https://ec.europa.eu/info/files/decision-adequate-protection-personal-data-republic-korea-annexes_en>.

[65] The Regulation of Processing of Personal Data (2021) is available at <http://documents.gov.lk/files/bill/2021/11/152-2021_E.pdf>.

[66] *See* https://www.bangkokpost.com/business/2110719/controversial-law-on-personal-data-againt-postponed-for-another-year.

[67] *See* Act No. 32 of 2018 Data Protection Act (12 July 2018), available athttps://www.bocra.org.bw/sites/default/files/documents/32%20Act%2010-08-2018-Data%20Protection.pdf and Data Protection Act (Commencement Date) Order, 2021 (15 October 2021).

[68] See Republic of Kenya, Office of the Data Protection Commissioner, "Guidance Note on access to personal date during Covid-19 pandemic" (January 2021), available at https://ict.go.ke/wp-content/uploads/2021/01/Draft-Data-Request-Review-Framework-Jan-2021.pdf.

[69] The FCCPC is empowered to administer and enforce provisions of every Nigerian law with respect to competition and protection of consumers under Section 17(a) of the Federal Competition and Consumer Protection Act, 2019.

[70] See "NITDA Collaborates With The Federal Competition And Consumer Commission (FCCPC) To Tackle Data Abuse By Money Lending Operations", Press Release (12 November 2021), available athttps://nitda.gov.ng/nitda-collaborates-with-the-federal-competition-and-consumer-commission-fccpc-to-tackle-data-abuse-by-money-lending-operations/.

[71] See "NITDA Sanctions SokoLoan For Privacy Invasion", Press Release (17 August 2021), available athttps://nitda.gov.ng/nitda-sanctions-soko-loan-for-privacy-invasion/.

[72] *See* Law No. 058/2021 Law relating to the protection of personal data and privacy (15 October 2021), available at https://www.minijust.gov.rw/fileadmin/user_upload/Minijust/Publications/Official_Gazette/_2021_Official_Gazettes/October/OG_Special_of_15.10.2021_Amakuru_bwite.pdf.

[73] *See* "Rwanda passes new Law protecting personal data", Press Release (21 October 2021), available at https://www.minict.gov.rw/fileadmin/user_upload/minict_user_upload/Documents/Press_Release/211021_PRESS_RELEASE_Rwanda_s_New_Data_Protection_Law_ENGLISH.pdf.

[74] *See* National Cyber Security Authority, "The Significance of Rwanda's Personal Data Protection and Privacy Law" (10 December 2021), available at https://cyber.gov.rw/updates/article/the-significance-of-rwandas-personal-data-protection-and-privacy-law-1/.

[75] *See* National Cyber Security Authority, "Consent, Ownership and Lawful Data Processing" (14 December 2021), available at https://cyber.gov.rw/updates/article/consent-ownership-and-lawful-data-processing-1/.

[76] *See* Section 110 of POPIA.

[77] *See* Information Regulator (South Africa), "Guidance Note on Processing of Special Personal Information" (June 2021), available at https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-Processing-SpecialPersonalInformation-20210628.pdf.

[78] *See* Information Regulator (South Africa), "Guidance Note On Exemptions From The Conditions For Lawful Processing Of Personal Information In Terms Of Section 37 And 38 Of The Protection Of Personal Information Act 4 Of 2013, 2021" (June 2021), available at https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-PPI-LawfulProcessing-202106.pdf.

[79] *See* Information Regulator (South Africa), "Rules of procedure relating to the manner in which a complaint must be submitted and handled by the Regulator, 2021" (October 2021), available at https://www.justice.gov.za/inforeg/legal/20211012-InfoReg-RulesOfProcedure-HandlingPOPIAcomplaints.pdf.

[80] *See* "Information Regulator to take further action regarding the WhatsApp privacy policy", Media Statement (13 May 2021), available at https://www.justice.gov.za/inforeg/docs/ms/ms-20210513-WhatsAppPrivacyPolicy.pdf.

[81] *See* Act No. 19 of 2020 Cybercrimes Act, 2020 (1 June 2021), available at https://www.gov.za/sites/default/files/gcis_document/202106/44651gon324.pdf.

[82] *See* "Togo : l'Assemblée nationale ratifie la convention de Malabo et actualise le fonctionnement de la CNDH" (in French) (14 July 2021), available at https://togomedia24.com/2021/07/01/togo-lassemblee-nationale-ratifie/.

[83] *See* Statutory Instrument No. 21 of 2021 The Data Protection and Privacy Regulations, 2021 (12 March 2021).

[84] *See* "Requirement to register with Personal Data Protection Office", Press Release (2 November 2021), available at https://www.linkedin.com/posts/personal-data-protection-office-pdpo_press-release-on-requirement-to-register-activity-6863366852064628736-wJc_.

[85] *See* Act No. 3 of 2021 The Data Protection Act, 2021 (24 March 2021).

[86] *See* Data Protection Act [Chapter 11:22].

[87] Bill (in Hebrew), available at https://documentcloud.adobe.com/link/review?uri=urn:aaid:scds:US:1510391d-592a-3272-bd12-d559164b70e2#pageNum=1.

[88] An unofficial translation of the Protection of Privacy Law, 5741 – 1981 is available at https://www.gov.il/BlobFolder/legalinfo/legislation/en/ProtectionofPrivacyLaw57411981unofficialtranslatio.pdf.

[89] Press Release (in Hebrew), available at https://www.gov.il/he/departments/news/amendments_privacy_protection_act.

[90] *See* "Iranian Hacking Group Leaks Patient and LGBTQ Info" (4 November 2021), available at https://www.infosecurity-magazine.com/news/iranian-hacking-group-leaks/.

[91] *See* "U.S. Department of the Treasury Announces Partnership with Israel to Combat Ransomware", Press Release (14 November 2021), available at https://home.treasury.gov/news/press-releases/jy0479.

[92] Announcement (in Hebrew), available at https://www.gov.il/he/departments/news/privacy_hod_hasharon_city.

[93] *See* "Israel to Share Vaccination Data With Pfizer as Part of Secret Deal" (10 January 2021), available at https://www.haaretz.com/israel-news/.premium-israel-to-share-covid-vaccine-data-with-pfizer-but-agreement-remains-secret-1.9438504, and a partially redacted version of the Real-World Epidemiological Evidence Collaboration Agreement, available at https://govextra.gov.il/media/30806/11221-moh-pfizer-collaboration-agreement-redacted.pdf.

[94] *See* "UAE adopts largest legislative reform in its history", Media Release, available at https://uaecabinet.ae/en/details/news/uae-adopts-largest-legislative-reform-in-its-history.

[95] The Data Protection Laws of UAE are available at https://u.ae/en/about-the-uae/digital-uae/data/data-protection-laws.

[96] *See* "ADGM enacts its new Data Protection Regulations 2021", Media Release (14 February 2021), available at https://www.adgm.com/media/announcements/adgm-enacts-its-new-data-protection-regulations-2021.

[97] *See* the dedicated website of the Office of Data Protection, available at https://www.adgm.com/operating-in-adgm/office-of-data-protection/overview.

[98] The Data Protection Guidance 2021, templates and assessments are available at https://www.adgm.com/operating-in-adgm/office-of-data-protection/guidance.

[99] Prime Minister's announcement (in Arabic), available at http://www.pm.gov.jo/content/1640846700/%D9%85%D8%AC%D9%84%D8%B3-%D8%A7%D9%84%D9%88%D8%B2%D8%B1%D8%A7%D8%A1-%D9%8A%D9%82%D8%B1%D9%91-%D9%85%D8%B4%D8%B1%D9%88%D8%B9-%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%AD%D9%85%D8%A7%D9%8A%D8%A9-%D8%A7%D9%84%D8%A8%D9%8A%D8%A7%D9%86%D8%A7%D8%AA-%D8%A7%D9%84%D8%B4%D8%AE%D8%B5%D9%8A%D9%91%D9%8E%D8%A9.html, and Ministry's announcement (in Arabic), available at https://modee.gov.jo/Ar/NewsDetails/%D9%82%D8%A7%D9%86%D9%88%D9%86_%D8%AD%D9%85%D8%A7%D9%8A%D8%A9_%D8%A7%D9%84%D8%A8%D9%8A%D8%A7%D9%86%D8%A7%D8%AA_%D8%A7%D9%84%D8%B4%D8%AE%D8%B5%D9%8A%D9%91%D9%8E%D8%A9_%D9%84%D8%B3%D9%86%D8%A9_2021%D9%85.

[100] The text of the draft law (in Arabic) is available at http://www.lob.jo/?v=1.14&url=ar/DraftDetails?DraftID:10254,AddComment:0,PageIndex:1&DraftTitle:%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%AD%D9%85%D8%A7%D9%8A%D8%A9-%D8%A7%D9%84%D8%A8%D9%8A%D8%A7%D9%86%D8%A7%D8%AA-%D8%A7%D9%84%D8%B4%D8%AE%D8%B5%D9%8A%D8%A9-/--%D8%AA%D9%85-%D8%AA%D9%85%D8%AF%D9%8A%D8%AF-%D9%85%D8%AF%D8%A9-%D9%86%D8%B4%D8%B1%D9%87-%D8%B9%D9%84%D9%89-%D8%A7%D9%84%D9%85%D9%88%D9%82%D8%B9-%D8%A7%D8%B1%D8%A8%D8%B9-%D8%A7%D9%8A%D8%A7%D9%85-%D8%B9%D9%85%D9%84-%D8%A7%D8%B6%D8%A7%D9%81%D9%8A%D8%A9.

[101] The Consultation Draft of the Personal Data Protection Bill 2021 (25 August 2021) is available at https://moitt.gov.pk/SiteImage/Misc/files/25821%20DPA%20Bill%20Consultation%20Draft_docx.pdf.

[102] *See* the announcement of the Qatar Financial Centre (QFC) Authority "Consultation on proposed changes to QFC Data Protections Regulations & Rules", available at https://www.linkedin.com/feed/update/urn:li:activity:6833700338965512192/, and the Consultation Paper "QFCA CP No. 1 of 2021 Proposed Changes to QFC Data Protection Regulations and Rules", available at https://qfcra-en.thomsonreuters.com/rulebook/qfca-cp-no-1-2021-proposed-changes-qfc-data-protection-regulations-and-rules.

[103] *See* "MOTC Releases Guidelines on Personal Data Privacy Protection Law", Media Release (31 January 2021), available at https://www.motc.gov.qa/en/news-events/news/motc-releases-guidelines-personal-data-privacy-protection-law.

[104] *See Personal Data Protection L*aw, implemented by Royal Decree M/19 of 17 September 2021 approving Resolution No. 98 (in Arabic) (14 September 2021), available at https://ncar.gov.sa/Documents/Details?Id=waEbJasbk9cJVNdJ%2B31GUA%3D%3D.

[105] *See* "The Communications Commission announces the entry into force of the Regulatory Framework for Cyber Security for Service Providers in the Communications, Information Technology and Postal Sector", Press Release (29 May 2021), available at https://www.citc.gov.sa/ar/mediacenter/pressreleases/Pages/20210529.aspx, and the Commission's portal on cybersecurity regulations, available at https://www.citc.gov.sa/ar/RulesandSystems/CyberSecurity/Pages/default.aspx.

[106] *See* https://www.gov.br/anpd/pt-br/assuntos/noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf.

[107] *See* https://www.gov.br/anpd/pt-br/assuntos/noticias/sancoes-administrativas-o-que-muda-apos-1o-de-agosto-de-2021.

[108] *See* https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-1-de-28-de-outubro-de-2021-355817513.

[109] *See* https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados/peticao-de-titular-contra-controlador-de-dados/reclamacao.

[110] *See* https://www.gov.br/mj/pt-br/assuntos/noticias/secretaria-nacional-do-consumidor-multa-banco-por-utilizar-dados-sem-consentimento-de-consumidores-idosos.

[111] *See* http://www.procon.mt.gov.br/-/17501890-procon-estadual-multa-rede-de-farmacias-por-infracao-a-lei-de-protecao-de-dados-pessoais.

[112] *See* http://www.bcra.gov.ar/Noticias/Ciberincidentes-lineamientos-para-respuesta-y-recuperacion.asp.

[113] *See* https://www.ciberseguridad.gob.cl/media/2021/11/Ciberguía-para-pymes.pdf.

[114] *See* https://www.dinardap.gob.ec/dos-anos-tienen-las-entidades-publicas-y-empresas-privadas-para-adaptar-sus-procesos-a-la-ley-de-proteccion-de-datos-personales/.

[115] *See* https://www.antai.gob.pa/reglamentan-ley-81-de-proteccion-de-datos-personales/.

[116] *See* http://silpy.congreso.gov.py/expediente/123459.

[117] *See* https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-23021 and https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-41021.

GIBSON DUNN

The following Gibson Dunn lawyers assisted in the preparation of this article: Alejandro Guerrero in Brussels; Ahmed Baladi, Vera Lukic, Clémence Pugnet, and Lena Bionducci in Paris; Connell O'Neil, Nicholas Hay, and Jocelyn Shih in Hong Kong; Kai Gesing in Munich; and Alex Southwell, Ryan Bergsieker, and Cassandra Gaedt-Sheckter in the United States.

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding these developments. Please contact the Gibson Dunn lawyer with whom you usually work, the authors, or any member of the firm's Privacy, Cybersecurity and Consumer Protection practice group:

Europe

Ahmed Baladi – Co-Chair, PCDI Practice, Paris (+33 (0)1 56 43 13 00, abaladi@gibsondunn.com)
James A. Cox – London (+44 (0) 20 7071 4250, jacox@gibsondunn.com)
Patrick Doris – London (+44 (0) 20 7071 4276, pdoris@gibsondunn.com)
Kai Gesing – Munich (+49 89 189 33 180, kgesing@gibsondunn.com)
Bernard Grinspan – Paris (+33 (0)1 56 43 13 00, bgrinspan@gibsondunn.com)
Penny Madden – London (+44 (0) 20 7071 4226, pmadden@gibsondunn.com)
Michael Walther – Munich (+49 89 189 33-180, mwalther@gibsondunn.com)
Alejandro Guerrero – Brussels (+32 2 554 7218, aguerrero@gibsondunn.com)
Vera Lukic – Paris (+33 (0)1 56 43 13 00, vlukic@gibsondunn.com)
Sarah Wazen – London (+44 (0) 20 7071 4203, swazen@gibsondunn.com)

Asia

Kelly Austin – Hong Kong (+852 2214 3788, kaustin@gibsondunn.com)
Connell O'Neill – Hong Kong (+852 2214 3812, coneill@gibsondunn.com)
Jai S. Pathak – Singapore (+65 6507 3683, jpathak@gibsondunn.com)

United States

Alexander H. Southwell – Co-Chair, PCDI Practice, New York (+1 212-351-3981, asouthwell@gibsondunn.com)
Debra Wong Yang – Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)
Matthew Benjamin – New York (+1 212-351-4079, mbenjamin@gibsondunn.com)
Ryan T. Bergsieker – Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)
Cassandra L. Gaedt-Sheckter – Palo Alto (+1 650-849-5203, cgaedt-sheckter@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)
H. Mark Lyon – Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com)
Karl G. Nelson – Dallas (+1 214-698-3203, knelson@gibsondunn.com)
Ashley Rogers – Dallas (+1 214-698-3316, arogers@gibsondunn.com)
Deborah L. Stein – Los Angeles (+1 213-229-7164, dstein@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)