GIBSON DUNN

February 1, 2021

INTERNATIONAL CYBERSECURITY AND DATA PRIVACY OUTLOOK AND REVIEW – 2021

To Our Clients and Friends:

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

Like many recent years, 2020 saw significant developments in the evolution of the data protection and cybersecurity landscape in the European Union ("**EU**"):

- On 16 July 2020, the Court of Justice of the EU ("**CJEU**" or "**Court**") struck down as legally invalid the EU-U.S. Privacy Shield, on which some companies relied to transfer personal data from the EU to the U.S. While companies are turning to other frameworks to transfer personal data, such as Standard Contract Clauses ("**SCCs**") and Binding Corporate Rules ("**BCRs**"), EU law also compels these companies to ensure that personal data will be safeguarded.

- As a consequence of the COVID-19 pandemic, a number of public, corporate and workplace practices have emerged to limit the spread of the virus, all which have privacy implications. To respond to this, many EU Member States have issued rules and guidelines with respect to the processing of personal data in the context of the pandemic.

- Negotiations among EU Member States have been ongoing regarding the adoption of a new e-Privacy Regulation, due to replace the soon 20-year-old e-Privacy Directive. Meanwhile, EU supervisory authorities have continued to publish guidance on cookie practices and other e-privacy matters, as well as to impose heavy fines on companies in breach of cookies-related requirements.

- Before Brexit was completed on 31 December 2020, the EU and the UK adopted the Trade and Cooperation Agreement, which includes an overall six-month "bridging mechanism" to cover transfers of personal data into the UK. The European Commission and the UK are in negotiations to adopt an adequacy decision that can enable the free flow of personal data beyond this six-month period, as in the pre-Brexit scenario.

In addition to the EU, different legal developments occurred in other jurisdictions around the globe, including in other European jurisdictions, the Asia-Pacific region, the Middle East, Africa and Latin America.

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

Table of Contents

I. European Union

A. International Data Transfers

1. The *Schrems II* Ruling
2. Guidance Adopted by the EDPB and Member State Authorities
3. Conclusions on Data Transfers

B. COVID-19 Pandemic

1. Guidance Adopted by Supervisory Authorities
2. Guidance at EU Member State Level
3. Next Challenges for the Fight against the COVID-19 Pandemic

C. E-Privacy and Cookies

1. Guidance Adopted by the EDPB and Member State Authorities
2. Reform of the e-Privacy Directive
3. Enforcement in Relation to Cookies

D. Cybersecurity and Data Breaches

1. Guidance and Initiatives Adopted by ENISA
2. Enforcement in Relation to Cybersecurity

E. The UK and Brexit 17

1. Transfers from and into the EU/EEA and the UK
2. Transfers from and into the UK and other Jurisdictions

F. Other Significant Developments in the EU

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

A. Russia

1. Access Restriction Trend in Privacy Laws Enforcement
2. The Russian Data Protection Authority Has Continued to Target Large, Multinational Digital Companies
3. Legislative Updates

B. Switzerland

1. The Revised FADP
2. The Swiss-U.S. Privacy Shield

C. Turkey

1. Turkish Data Protection Authority and Board Issues a Number of Regulations, Decisions and Guidance Documents
2. Turkish Data Protection Act Continues to be Enforced

III. Developments in Asia-Pacific, Middle East and Africa

A. Australia

B. China

1. New Developments in Chinese Legislation
2. Enforcement of Chinese Data Protection and Cybersecurity Legislation

C. Hong Kong SAR

D. India

1. Legislative initiatives
2. Regulatory opinions and guidance
3. Enforcement of data protection laws

E. Indonesia

F. Israel

G. Japan

H. Malaysia

I. Singapore

J. South Korea

K. Thailand

L. United Arab Emirates

M. Other Developments in Africa

N. Other Developments in the Middle East

O. Other Developments in Southeast Asia

IV. Developments in Latin America and in the Caribbean Area

A. Brazil

B. Other Developments in South America

1. Argentina
2. Chile
3. Colombia
4. Mexico
5. Uruguay

I. European Union

A. International Data Transfers

1. The Schrems II Ruling

On 16 July 2020, the CJEU struck down as legally invalid the EU-U.S. Privacy Shield, which some companies had relied upon to transfer personal data from the EU to the U.S. The Court also ruled that the Standard Contractual Clauses ("**SCCs**") approved by the European Commission, another mechanism used by many companies to transfer personal data outside of the EU, remained valid with some caveats. The Court's landmark decision has forced companies on both sides of the Atlantic to reassess their data transfer mechanisms, as well as the locations where they store and process personal data.[1]

2. Guidance Adopted by the EDPB and Member State Authorities

Following the *Schrems II* ruling, several supervisory authorities shared their views and opinions on its interpretation.[2] On its side, the UK Information Commissioner's Office ("**ICO**") invited companies to continue transferring data on the basis of the invalidated Privacy Shield and, on the contrary, several German Authorities have advised against it.

These initial reactions were overcome by the Frequently Asked Questions **("FAQ")** report issued by the European Data Protection Board ("**EDPB**") on 23 July 2020. In its FAQs on *Schrems II*, the EDPB stated, in particular, the following:

i. No "grace" period is granted for entities that relied on the EU-U.S. Privacy Shield. Entities relying on the now invalidated Privacy Shield should immediately put in place other data transfer mechanisms or frameworks.

ii. Data controllers relying on SCCs and BCRs to transfer data should contact their processors to ensure that the level of protection required by EU law is respected in the third country concerned. If personal data is not adequately protected in the importing Member State, the controller or the processor responsible should determine what supplementary measures would ensure an equivalent level of protection.

iii. If data transferred cannot be afforded a level of protection essentially equivalent to that guaranteed by EU law, data transfers should be immediately suspended. Companies willing to continue transferring data under these circumstances should notify the competent supervisory authority(ies).[3]

In October 2020, the U.S. Department of Commerce and the European Commission announced that they had initiated discussions to evaluate the potential for a new version of the Privacy Shield that would be compliant with the requirements of the *Schrems II* ruling.[4]

Pending the discussions between the EU and the U.S. on a new data transfer framework, on 10 November 2020, the EDPB issued important new guidance on transferring personal data out of the EEA, namely:

i. **Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data**,[5] which aim to provide a methodology for data exporters to determine whether and which additional measures would need to be put in place for their transfers; and

ii. **Recommendations 02/2020 on the European Essential Guarantees ("EEG") for surveillance measures**,[6] which aim to update the EEG, in order to provide elements to examine whether surveillance measures allowing access to personal data by public authorities in a receiving country, whether national security agencies or law enforcement authorities, can be regarded as a justifiable interference.

The EDPB's guidance lessened some of the uncertainty caused by the *Schrems II* ruling. However, since this guidance was issued in the form of a public consultation closing on 21 December 2020, it may be subject to further changes or amendments.

In the Recommendations on supplementary transfer tools, the EDPB recommends that data exporters: (i) map all transfers of personal data to third countries and verify that the data transferred is adequate, relevant and limited to what is necessary; (ii) verify the transfer tool on which the transfers are based; (iii) assess whether there is anything in the law or practice of the third country that may impinge on the effectiveness of the appropriate safeguards, and document this assessment; (iv) identify and adopt additional measures (examples are provided in Annex 2 of the Recommendations); (v) take any formal procedural steps that the adoption of the supplementary measure may require; and (vi) re-evaluate at appropriate intervals the level of protection afforded to the data transferred. Although the guidance takes the form of non-binding recommendations, companies that transfer personal data outside of the EEA would be well served to review their approach to such transfers in light of the EDPB guidance.

On 12 November 2020, the European Commission published a draft implementing decision on SCCs for the transfer of personal data to third countries along with a draft set of new SCCs. The new SCCs include several modules to be used by companies, depending on the transfer scenario and designation of the parties under the GDPR, namely: (i) controller-to-controller transfers; (ii) controller-to-processor transfers; (iii) processor-to-processor transfers; and (iv) processor-to-controller transfers.

These new SCCs also incorporate some of the contractual supplementary measures recommended by the EDPB, as described above. They have been opened for public consultation that closed on 10 December 2020 and the final new set of SCCs is expected to be adopted in early 2021. At this stage, the draft provides for a grace period of one year during which it will be possible to continue to use the old SCCs for the execution of contracts concluded before the entry into force of the new SCCs.[7]

Besides, the European Commission also published on 12 November 2020 draft of SCCs for contracts between controllers and processors. These SCCs are intended to be optional (the parties may choose to continue using their own data processing agreements) and have also been opened for public consultation that closed on 10 December 2020. The final draft of SCCs are also expected to be adopted in early 2021.[8]

On 15 January 2021, the EDPB and European Data Protection Supervisor adopted joint opinions on both sets of SCCs (one opinion on the SCCs for contracts between controllers and processors, and another one on SCCs for the transfer of personal data to third countries).[9]

3. Conclusions on Data Transfers

As explained above, 2020 was a year of changes when it comes to data transfer mechanisms.

The EU-U.S. Privacy Shield, once believed to have put an end to the issues raised by the EU-U.S. Safe Harbour, has again been deemed to be insufficient to safeguard the data protection rights of individuals in the EU. It is expected that, with a change in the U.S. federal administration, and the need for authorities to give legal certainty and facilitate cross-border commercial activity in the current economic context, the EU and the U.S. will work swiftly towards a mechanism that can resolve transatlantic transfers once and for all.

The adoption of new SCCs, expected to occur in 2021, will also bring more certainty to companies that relied on this framework to transfer personal data. The new sets of SCCs will cover wider scenarios than those under the current framework, reducing implementation costs and limiting uncertainty. However, given the limited grace period expected to apply to pre-GDPR SCCs, and the introduction of changes to the new SCCs, companies should take the opportunity to review the new contractual framework and adapt it to their data transfer needs.

B. COVID-19 Pandemic

The COVID-19 pandemic and the ensuing health crisis has led to the emergence of new practices to limit the spread of the virus, such as the issuance of tracing apps and the implementation of temperature checks at public administration buildings or at the workplace. These practices involve the processing of various health data, and may therefore have privacy implications. On the other hand, remote working has increased the exposure of companies and their employees to cybersecurity risks, such as the use of private (unprotected and non-certified) assets to review, print or process company information.[10]

1. Guidance Adopted by Supervisory Authorities

On 19 March 2020, the EDPB adopted a statement on the processing of personal data in the context of COVID-19. In the statement, the EDPB emphasised that while data protection rules should not hinder the fight against the virus, data controllers and processors must ensure the protection of personal data even in these exceptional times.[11]

Further, on 17 April 2020, the European Commission set out the criteria and requirements that applications supporting the fight against COVID-19 must meet in order to ensure compliance with data protection regulations.[12] Building on this guidance, the EDPB adopted Guidelines on geolocation and other tracing tools in the context of the COVID-19 outbreak as well as Guidelines on the processing of health data for research purposes in the context of the COVID-19 outbreak.[13]

Since the beginning of the pandemic, European authorities have also focused on pooling resources at the EU level. The European Commission and the EDPB published materials relating to the interoperability between the Members States' contact tracing applications, in order for users to be able to rely on a single app wherever they are located in the EU.[14]

The EDPS also issued a Preliminary Opinion on the European Health Data Space, which aims to promote better exchange and access to different types of health data within the EU.[15]

2. Guidance at EU Member State Level

Member State supervisory authorities have also issued their own guidance with respect to the processing of personal data in the context of the COVID-19 pandemic. Although authorities have emphasised the general principles set forth under the GDPR, they have failed to adopt a unified approach.

As regards national tracing applications, the UK ICO issued a notice on the joint initiative by two tech companies to enable the use of Bluetooth technology in contact research applications,[16] as well as on the development of contact tracing applications in accordance with the principles of privacy by design and privacy by default.[17] In France, the French supervisory authority (the "**CNIL**") opened and closed a formal enquiry into the national tracing app sponsored and developed by the French government,[18] after requesting the Ministry of Solidarity and Health to remedy certain breaches identified in the app.[19] In Germany, as in France, the authority emphasised that the use of the national COVID-19 app should be voluntary.[20]

On a different note, supervisory authorities have also intervened in different degrees in the testing and tracing efforts of public authorities. In the UK, for example, the ICO issued a notice on the recording and retention of personal data in support of the test and trace scheme, where it advised in particular to only collect data requested by the government, not to reuse the data for other purposes, and to delete the data as soon as it is no longer necessary.[21] In Germany, a regional supervisory authority even issued warnings for excessive health requests.[22]

Supervisory authorities have also issued substantial guidance in respect of measures to fight the COVID-19 pandemic in an employment context, for example, in the UK,[23] France,[24] Italy,[25] Belgium[26] and the Netherlands.[27] The topics covered by supervisory authorities include the implementation of tests and the monitoring of employees, the reporting of sensitive information to the employer, and in turn the communication of such information to the health authorities, as well as remote work.

The use of smart and thermal cameras has also been strictly regulated both in France and in Germany.[28]

3. Next Challenges for the Fight against the COVID-19 Pandemic

While data protection laws were not meant to hinder the deployment of necessary measures to trace and contain the evolution of the virus, EU supervisory authorities have been adamant that this should not come at a cost in terms of privacy.

Privacy standards are likely to remain high as Member States commence their vaccination plans and prepare for the post-COVID-19 economic recovery. For example, in the Member States the monitoring of doses and medical supervision of patients are generally conducted by qualified medical staff, and health and pharmaceutical institutions. However, there is still some debate whether private and public institutions can issue or request vaccination "passports" or certificates to facilitate the safe movement of people.[29] With regard to tracing and detection data, public administrations and companies have to assess the proper retention periods that apply to the storage and archive of such information.

C. E-Privacy and Cookies

Against the backdrop of the ongoing EU discussions on the future e-Privacy Regulation, guidance has been released by Member State supervisory authorities. Meanwhile, significant fines continue to be imposed on companies that do not comply with applicable e-privacy rules.

1. Guidance Adopted by the EDPB and Member State Authorities

On 5 April 2020, the EDPB updated its Guidelines (05/2020) on consent, which now specifically address the practice of so-called "cookie walls" (a practice which consists in making access to online services and functionalities conditional on the consent of a user to cookies). Among others, in these Guidelines the EDPB explicitly states that continuing browsing on a website does not meet the requirements of valid consent.[30]

As a result of the additional clarifications provided by the EDPB, the **Spanish supervisory authority** ("**AEPD**") updated its guidance on the use of cookies, denying the validity of consent obtained through cookie walls or continued browsing.[31]

In **France**, the CNIL adopted a different approach set by the French Administrative Court, which in a 2020 ruling invalidated the general and absolute ban on cookie walls. Consequently, the CNIL adopted amending guidelines and a recommendation on the use of cookies and other tracing devices, offering practical examples of the collection of user's consent.[32]

2. Reform of the e-Privacy Directive

The e-Privacy Regulation was proposed by the European Commission in 2017 in order to update the legislative rules applicable to digital and online data processing and to align e-privacy laws to the GDPR. Ambitious and promising at first, eight presidencies of the Council of the EU have been unable to push the project over the finish line.

In January 2021, the Portuguese Presidency of the Council of the EU (January to June 2021) proposed a new version (the 14th) of the e-Privacy Regulation, with the aim to simplify the text and further align it with the GDPR.[33]

While the new Regulation is not expected to be applicable before 2022, its adoption process should be closely monitored in order to anticipate compliance efforts that will be required, in particular in view of the shorter transition period (from 24 to 12 months) set out in the proposal of the Portuguese Presidency.

3. Enforcement in Relation to Cookies

In parallel, Member State supervisory authorities continued to enforce their national e-privacy legislation transposing the e-Privacy Directive.

In **Spain**, a social network service was fined €30,000 for breaching the rules relating to cookies, specifically because its cookie banner did not enable users to reject the use of trackers or to issue consent per type of cookie.[34] Similarly, the AEPD imposed a fine of the same amount to an airline for implementing a "cookie wall" on its website.[35]

In **France**, hefty fines have been imposed for violations of the legal provisions on cookies. First, two companies of a food and goods retail distribution group were fined €2,250,000 and €800,000 euros for various violations, including the automatic setting of cookies on users' terminals.[36] More recently, two U.S. tech companies have been imposed fines of €100 million and €35 million, respectively, due to violation of the legal framework applicable to cookies. In particular, the CNIL observed that these companies placed advertising cookies on user's computers without obtaining prior consent and without providing adequate information.[37]

D. Cybersecurity and Data Breaches

As in previous years, EU and Member State supervisory authorities and cybersecurity agencies have continued to be active in the adoption of measures and decisions that enhance and enforce cybersecurity standards.

1. Guidance and Initiatives Adopted by ENISA

The EU Agency for Cybersecurity ("**ENISA**") has the mandate of increasing the protection of public and private networks and information systems, to develop and improve cyber resilience and response capacities, and to develop skills and competencies in the field of cybersecurity, including management of personal data.

In 2020, ENISA continued to issue guidelines and to spearhead initiatives to achieve these objectives:

- On 27 January 2020, ENISA released an online platform to assist companies in the security of personal data processing. Among others, the platform focuses on the analysis of technical solutions for the implementation of the GDPR, including the principle of privacy by design. The platform may assist data controllers and processors in the determination of their approach when developing personal data protection policies.[38]

- On 4 February 2020, ENISA published a report outlining frameworks, schemes and standards of possible future EU cybersecurity certification schemes. The report focuses in particular on the current standards applied to fields such as the Internet of Things, cloud infrastructure and services, the financial sector and electronic health records. The Report also addresses gaps in the current cybersecurity certification schemes, paving the way for the adoption of future EU cybersecurity certification schemes.[39]

- On 19 March 2020, ENISA issued a report on security requirements for digital service providers and operators of essential services, based on Directive (EU) 2016/1148 of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union ("NISD") and the GDPR. Among other things, the report proposes and sets the outline for a risk-based approach to security. It identifies the guidelines relevant to NISD and GDPR security measures, recommends the establishment of certification mechanisms, and sets the need for competent EU bodies and research bodies to continue providing specialised guidance on state-of-the-art data protection and security techniques.[40]

- On 9 June 2020, ENISA made available a visual tool to ensure transparency with regard to cybersecurity incidents. The tool provides information on eight years of telecommunications security incidents, as well as four years of trust services incident reports. In total, the tool provides information on a total of 1,100 cybersecurity incidents notified as mandated by EU legislation for over nine years. In its release, ENISA noted that, over the last four years, system failure was the most common cause behind both telecom security incidents and trust services incidents.[41]

Finally, it is worth noting the Strategy for a Trusted and Cyber Secure Europe released by ENISA on 17 July 2020. The Strategy aims to achieve a high common level of cybersecurity across the EU, containing ENISA's strategic objectives to boost cybersecurity, preparedness, and trust across the EU. The Strategy sets out a list of seven objectives that it aims to reach, including the effective cooperation amongst operational actors within the EU in case of massive cyber incidents, the creation of a high level of trust in secure digital solutions, and efficient and effective cybersecurity information and knowledge management for Europe.[42]

2. Enforcement in Relation to Cybersecurity

Member State supervisory authorities have been particularly active in sanctioning data breaches and the lack of appropriate security measures, with significant monetary penalties.

For example, in the **UK**, three sanctions have been especially significant. *First*,an airline company was fined £20 million following a cyberattack in 2018, compromising the personal and financial data of more than 400,000 of its customers for over two months.[43] ICO investigators found that the airline company should have identified weaknesses in its security and resolved them with security measures that were available at the time, which would have prevented the cyber-attack.

Second, a hotel chain was fined £18.4 million after an estimated 339 million guest records worldwide were affected following a cyberattack that occurred in 2014, but remained undetected until September 2018.[44] According to the ICO, the investigation revealed failures on the side of the hotel chain to put appropriate technical or organisational measures in place to protect the personal data being processed on its systems, as required by the GDPR. In those two cases, the ICO significantly reduced the amount of the fine originally considered in its notice of intention to fine the companies, taking into account the company's representations and the economic impact of the COVID-19 pandemic in setting the final amount of the fine.

Third, a ticket sales and distribution company was imposed a £1.25 million fine for failing to comply with its security obligations, in the context of a cyberattack on a chatbot installed on its online payment page, potentially affecting the data of 9.4 million people.[45] The ICO concluded that the company failed to assess the risks of using a chat-bot on its payment page, identify and implement appropriate security measures to negate the risks, and identify the source of suggested fraudulent activity in a timely manner.

In **Germany**, a German telecommunications service provider was fined by the German Federal Data Protection Authority for insufficient data security procedures established in a call centre that lead to an inappropriate disclosure of a cell phone number of an individual who then complained to a data protection authority. While the fine initially amounted to €9.5 million, it was challenged by the telecommunications service provider and later reduced by the competent district court in Bonn to €900,000.

More recently, in **Ireland**, a social network service was fined €450,000 concerning its 2019 data breach. This decision bears great importance, as it represented the outcome of the first application of the GDPR dispute resolution mechanism, where the Irish Data Protection Commission adopted a decision further to the adoption of a prior decision by the EDPB.[46]

On 30 July 2020, the **Council of the EU** imposed its first ever sanctions on cyberattacks. In particular, the Council adopted restrictive measures against six individuals and three entities responsible for or involved in various cyberattacks, including a travel ban and an asset freeze. In addition, EU individuals and entities are forbidden from making funds available to these individuals and entities.[47]

E. The UK and Brexit

The UK regained full autonomy over its data protection rules at the end of the Brexit transition period, on 31 December 2020. However, before Brexit was concluded, the EU and the UK entered into the EU-UK Trade and Cooperation Agreement on 30 December 2020.[48] This Agreement regulates data flows from the EU/EEA to the UK under a so-called "bridging mechanism", and sets a timeline for the adoption of an EU-UK adequacy decision thereafter.

The Trade and Cooperation Agreement includes mechanisms to enable the UK to make changes to its data protection regime or exercise international transfer powers, subject to mutual agreement, without affecting the bridging mechanism. The EU does not have the power to block changes to the UK's framework or use of its powers. However, if the EU objects to changes considered by the UK, and the UK implements them despite these objections, the EU/EEA-UK bridge will be terminated.

1. Transfers from and into the EU/EEA and the UK

As indicated above, the bridging mechanism contained in the EU-UK Trade and Cooperation Agreement covers **personal data transfers from the EU/EEA to the UK**. According to the provisions in the Agreement, it will apply for up to a maximum period of six months, unless an adequacy decision comes into effect earlier. The adoption of an EU adequacy decision for the UK, which is expected to be adopted

in 2021, would enable the ongoing free flow of personal data from the EEA to the UK thereafter, without needing to implement additional safeguards.

Notwithstanding the stability offered by the Trade and Cooperation Agreement, the UK Government has advised companies to put in place alternative transfer mechanisms that may safeguard personal data received from the EEA against any interruption to the free flow of personal data.[49] SCCs have been identified as the most relevant mechanism that organisations may resort to in order to safeguard such transfers.

On the other side, regarding **personal data transfers from the UK to the EU/EEA and Gibraltar**, the conditions under which such transfers may be made will remain unchanged and unrestricted, according to the UK Government.[50]

2. Transfers from and into the UK and other Jurisdictions

The transfer of personal data from third countries and territories to the UK generally raises questions of legal compliance in the exporting jurisdiction. The impact of Brexit has been particularly significant regarding the regulation of data transfers into the UK from jurisdictions that were already covered by an adequacy decision of the European Commission.

Pre-Brexit, the European Commission had made findings of adequacy of personal data transfers to a number of jurisdictions.[51] These adequacy decisions generally address the inbound transfer of personal data from these jurisdictions into the EU/EEA. However, in order to obtain and maintain these adequacy decisions, these jurisdictions put in place legal restrictions on (onward) transfers of personal data to countries outside the EEA, which now include the UK.

To resolve potential issues on transfers of personal data from these jurisdictions to the UK, the governments of most of these jurisdictions have issued statements, resolutions and even modified their legal regimes in order to permit the continued transfer of personal data into the UK. The UK ICO has indicated that it is continuing to work with these jurisdictions in order to make specific arrangements for transfers of personal data to the UK.[52]

On the UK side, the 2019 Brexit regulations applicable to data protection matters recognised the European Commission's adequacy decisions, and rendered permissible cross-border transfers of personal data to these jurisdictions.[53] The Government and the ICO are working on the adoption of new UK adequacy regulations, to confirm that particular countries, territories or international organisations ensure an adequate level of protection, so as to allow transfers of personal data from the UK to these jurisdictions, without the need for adoption of additional safeguards. SCCs and other mechanisms for lawful international data transfers may be put in place to cover transfers of personal data from the UK to jurisdictions not covered by adequacy decisions.

F. Other Significant Developments in the EU

More generally, this year has been marked by the adoption of important **EDPB Guidelines**. In addition to those mentioned above, the EDPB released new Guidelines on the concepts of controller and processor, on the targeting of social media users, and on data protection by design and by default.[54]

Furthermore, hefty fines were imposed as mentioned in Sections I.A to D above, in particular in **France** with the €100 million fine imposed on a tech company which is the highest penalty ever imposed by a supervisory authority as of end of December 2020.

Fines were also imposed on topics other than those addressed above. In particular, in **Germany**, the Hamburg supervisory authority fined a retail company €35.3 million for illegally collecting and storing sensitive personal data from employees, such as information about health condition, religious beliefs and family matters. According to the authority's investigation, data about the personal life of the company's employees had been collected comprehensively and extensively by supervisors since at least 2014, and stored on the company's network drive. This information was accessible to up to 50 managers of the company and was used, among other things, to create profiles of individual employees in order to evaluate their work performance and to adopt employment decisions. In sum, the practice of the company amounted to a number of data protection violations, including a lack of legal basis for the data processing, illegal processing of the data, and the absence of controls to limit storage and access to the data.[55]

Significant monetary penalties have also been imposed due to the lack of valid consent under the GDPR:

- In **Italy**, two telecommunications operators were fined approximately €17 and €12 million for processing hundreds of unsolicited marketing communications without having obtained users' prior consent, without having offered to users their right to object to the processing, and for aggressive telemarketing practices, respectively.[56]

- In **Spain**, the AEPD fined a bank €5 million for violations of the right to information and for lack of valid consent. In particular, the bank used imprecise terminology to define the privacy policy, and provided insufficient information about the category of personal data processed, especially in relation to customer data obtained through financial products, services, and channels. Moreover, the bank failed to obtain consent before issuing promotional SMS messages, and did not have in place a specific mechanism for consent to be obtained by customers and account managers.[57]

As regards the requirements for valid consent under the GDPR, the **CJEU**, in its ruling on *Orange România SA v Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal*, decided that valid consent cannot be inferred from a preselected box in a contract for the provision of telecommunications services, whereby the customer allegedly consents to the collection and storage of his/her identity document. The Court specified that this is also the case where the customer is misled as to the possibility of concluding the contract if he/she refuses to consent to the processing of his/her data, or where the freedom to choose to object to that collection and storage is affected by the requirement to complete an additional form setting out that refusal.[58]

In addition to increased scrutiny by data protection authorities, there is also a slightly increasing trend in private enforcements actions from consumers and (former) employees. These actions primarily relate to both the enforcement of transparency and access rights to personal data as well as claims for compensation for alleged GDPR violations.

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

As explained in the 2020 International Outlook and Review, the increasing impact of digital services in Europe and the overhaul brought about by the GDPR in the EU have continued to influence the regulatory and enforcement actions of jurisdictions in the vicinity of the EU.

A. Russia

1. Access Restriction Trend in Privacy Laws Enforcement

Russian local data privacy laws have continued to be heavily enforced by the Russian Federal Service for the Supervision of Communications, Information Technology and Mass Communications ("**Roskomnadzor**"). This activity reflects the growing priority and concern that personal data protection represents for the Russian population. According to Roskomnadzor's statistics, in the previous year the number of complaints concerning personal data protection had increased to 50,300. The largest number of complaints related to the actions of the owners of internet sites, including social networks, credit institutions, housing and communal services organisations, and collection agencies.[59]

The most notable activity of Roskomnadzor in 2020 was its use of its regulatory powers to manage activities of numerous Internet-based services. Below we describe three noteworthy cases where the access to Internet resource was restricted by Roskomnadzor until the respective company satisfied certain expectations and /or requests of the regulator.

On 29 January 2020, Roskomnadzor announced that it would restrict access to the mail service of a tech company. In deciding so, Roskomnadzor noted that the company was used by cybercriminals to send false messages under the guise of reliable information, and that it had categorically refused Roskomnadzor's repeated requests for information to be included in the register of information dissemination organisers on the Internet.[60] However, the company has taken actions to address the situation, and currently it is accessible for the Russian users.

On 20 February 2020, Roskomnadzor took a similar measure and temporarily restricted access to another email service provider.[61] The authority stated that, in 2019 and in February 2020, the email service had been used by cyber-attackers to send false messages under the guise of reliable information about the massive mining of social transport infrastructure and ships in the Russian Federation.

On 18 June 2020, Roskomnadzor also announced that it had removed the requirements to restrict access to the messaging application of a tech company.[62] This decision was paired with Roskomnadzor's declaration of its readiness to cooperate with internet companies operating in Russia to quickly suppress the spread of terrorist and extremist information, child pornography, and the promotion of suicide and drugs. In addition, Roskomnadzor noted that, through joint efforts with leading Russian and foreign

companies, it had removed, on average and weekly, 2,500 materials relating to suicidal behaviours, 1,300 materials of an extremist and terrorist nature, 800 materials propagandising drug use, and 300 materials containing pornographic images of minors.

2. The Russian Data Protection Authority Has Continued to Target Large, Multinational Digital Companies

In 2020, Roskomnadzor followed its set trend in targeting large, multinational digital companies. On 31 January 2020 the authority announced that it had initiated administrative proceedings against two social network services.[63] In particular, Roskomnadzor stated that these companies did not meet the requirements for data localisation of Russian users on servers located in the Russian Federation.

Following the authority's proceedings, on 13 February 2020, the Tagansky District Court of Moscow fined both social network services RUB 4 million (approx. €45,000) for these violations.[64] The Court affirmed the authority's finding that one of the companies had violated Russia's legal requirement to record, organise and store the personal data of Russian citizens in databases located in the Russian Federation.[65]

3. Legislative Updates

Several notable laws have been adopted at the end of 2020.

New amendments to the Code of Administrative Offenses of the Russian Federation entail considerable fines for failure to delete prohibited information upon the request of Roskomnadzor.[66] The fines can be imposed on hosting providers or any person enabling other persons to publish information on the Internet for failure to restrict access to prohibited information and owners of the websites or Internet resources for non-deletion of prohibited information may be up to RUB 4,000,000 (approx. €45,000) for the first offence and up to 10% of the company's annual turnover from the preceding calendar year (but not less than RUB 4,000,000) for the subsequent offence. If prohibited information contains propaganda of extremism, child pornography, or drugs, liability is increased for up to RUB 8,000,000 (approx. €90,000) for the first offence or up to 20% of the company's annual revenue from the preceding calendar year (but not less than RUB 8,000,000) for the subsequent offence. This law is aimed at establishing liability for hosting providers, owners of websites and information resources who fail to restrict access to or delete the information, dissemination of which is prohibited in Russia, and has come into force on 10 January 2021.

Another amendment to Russian law[67] increases significantly the risks of blocking of internet resources in Russia. The law introduces the status of the owner of an Internet resource involved in violations of the fundamental human rights of Russian citizens. The Prosecutor General, in consultation with the Russian Foreign Ministry, may assign this status to the owner of an Internet resource that discriminates against materials from the Russian media. Such a decision can be made if the internet resource limits access to socially important information based on the nationality, language, or in connection with the imposition of sanctions against Russia or its citizens. If the owner of the internet resource censors or anyhow restricts the access to accounts of Russian media, Roskomnadzor is entitled to restrict access to such internet resource, fully or partially. This law has come into force on 10 January 2021.

The law amending the Personal Data Law significantly changes the legal landscape with regard to the processing of publicly available personal data.[68] As per the new law, data controllers making personal data publicly available for further processing by third parties must obtain individuals' explicit consents, which shall not be bundled to any other consents and data subjects have a wide range of rights in this regard.

Third parties who intend processing publicly available personal data have three options: (i) to rely on the consent obtained by the controller when making the data publicly available, subject to compliance with the rules of data processing; (ii) to rely on the consent provided by an individual to Roskomnadzor via a dedicated web-based platform to be set up under the law, but also subject to compliance with the rules of data processing; or (iii) to ensure on their own that they have appropriate legal grounds as per the general requirements of Russian Personal Data Law. The above rules will enter into force as of 1 March 2021.

In addition, the new law introduces the data controller's obligation to publish information on the processing terms and existing prohibitions and conditions for processing of personal data, permitted by a data subject for dissemination, by an unlimited number of persons. These new requirements will come into force as of 1 July 2021. According to the amendments to the Law on Information, Information Technologies, and Information Protection, if a resource is considered a social network, it will be included in the register maintained by the Roskomnadzor.[69] These amendments impose moderation obligations on social networks regarding the content published by users, and require them to make available certain information on their websites.

In practice, social networks will now be required to identify and restrict access to illegal content.[70] Furthermore, the following information must be posted on the social network by its owner: (i) name, email address and an electronic form for sending requests about the illegal content; (ii) annual reports on the results of the consideration of requests and monitoring activities; (iii) terms of use of the social network. This amendment will enter into force on 1 February 2021.

The recently adopted laws evidence the trend of the increased regulation of IT-industry activities in Russia. With these new regulations, the Russian authorities increase the regulatory mechanisms that may affect the activities of websites, news media, social media, social networks and video hosting services in Russia.

B. Switzerland

1. The Revised FADP

On 25 September 2020, the Swiss Parliament adopted the revised version of the Federal Act on Data Protection 1992 ("**Revised FADP**").[71] The Revised FADP is not in force yet, as it was subject to approval by referendum until 14 January 2021 (which was not held). The Federal Council will decide on entry into force which is expected during 2021 or at the beginning of 2022. The specific date is particularly important because the Revised FADP does not provide for any transitional periods.

One of the main reasons behind the adoption of the Revised FADP was to ensure that the EU recognises Switzerland as providing an adequate level of protection to personal data according to GDPR standards.

The most significant differences between the Revised FADP and the previous version, are the following:

- The Revised FADP now codifies expressly the international principle of the effects doctrine, subject to the principles governing civil and criminal enforcement that remain in place.[72] Hence, the Revised FADP will also apply on persons that are domiciled outside of Switzerland if they process personal data and this data processing has an effect in Switzerland.

- Personal data pertaining to legal entities is no longer covered by the Revised FADP, which in line with the GDPR, and most foreign data protection laws.[73]

- The Revised FADP will extend the term of sensitive data by adding two new categories: (i) genetic data; and (ii) biometric data that uniquely identifies an individual.[74]

- The Revised FADP now contains a legal definition of profiling that corresponds to the definition in the GDPR.[75]

- The Revised FADP distinguishes controllers and processors.[76]

- Like the GDPR, the Revised FADP contains provisions concerning data protection by design and by default.[77]

- The Revised FADP provides that a processor can hire a sub-processor only with the prior consent of the controller.[78]

- Under the Revised FADP and subject to specific exemptions, controllers and processors must maintain records of data processing activities under their respective responsibility. The former duty to notify data files to and register with the Federal Data Protection and Information Commissioner ("**FDPIC**") has been abolished.[79]

- Under the Revised FADP and under specific conditions, controllers that are domiciled or resident abroad and process personal data of Swiss individuals must designate a representative in Switzerland.[80]

- The Revised FADP provides that individuals must (at the time of collection) be informed about certain minimum information[81] and have a new right to intervene in case of automated decision-making.[82]

- Under the Revised FADP, the FDPIC will have the power to issue binding decisions. However, it will not have the unilateral power to impose fines, unlike most data protection authorities in Europe – resort to Swiss courts will be required.

- Controllers are required to conduct a Data Protection Impact Assessment ("**DPIA**") where there is a high risk for the privacy and the fundamental rights of data subjects.[83]

- Controllers will have a data breach notification obligation to the FDPIC where an incident results in high risk for data subjects.[84]

- The Revised FADP introduces the right to data portability, which was not covered by the previous data protection law.[85]

- The maximum amount of sanctions for individuals will be CHF 250,000 (approx. €232,000),[86] and the Revised FADP also extends criminal liability to the violation of additional data protection obligations.

As can be seen, there are significant similarities between the Revised FADP and the GDPR. The entry into force of the Revised FADP is therefore expected to lead to continuity in the cross-border data transfers between the EU and Switzerland.

2. The Swiss-U.S. Privacy Shield

On 8 September 2020, the FDPIC published an assessment on the Swiss-U.S. Privacy Shield where it found that the cross-border transfer mechanism did not guarantee an adequate level of protection regarding data transfers from Switzerland to the U.S.[87] Prior to FDPIC's assessment, the CJEU had delivered its judgment in *Schrems II*,[88] in July 2020, which rendered the European Commission's decision on the EU-U.S. Privacy Shield invalid.

The FDPIC identified two key problems concerning the Swiss-U.S. Privacy Shield, namely: (i) the lack of an enforceable legal remedy for persons concerned in Switzerland in particular due to the inability to assess the effectiveness of the Ombudsman mechanism because of a lack of transparency; and (ii) the inability to assess the decision-making abilities of the Ombudsman and its independence with respect to U.S. intelligence services. Since FDPIC's assessment is a soft-law instrument without legally binding nature, the Swiss-U.S. Privacy Shield will remain valid and binding for the companies registered unless and until it is repealed or annulled on a case-by-case basis by the competent Swiss courts or in its entirety by the U.S.

C. Turkey

1. Turkish Data Protection Authority and Board Issues a Number of Regulations, Decisions and Guidance Documents

In 2020, the Turkish Data Protection Authority ("**KVKK**") and the Turkish Data Protection Board (the "Board") continued to issue a number of statements, decisions and guidance documents regarding the application and enforcement of Turkish data protection provisions. We outline and briefly explain below the most relevant ones:

- On 16 December 2020, the KVKK issued a statement on the data protection rules related to publicly available personal data. In the statement, the KVKK acknowledged that the Law on Protection of Personal Data No. 6698 ("**Turkish Data Protection Act**") allows personal data to be processed where the data concerned is made available to the public by the data subject themselves.[89] However, the KVKK clarified that the concept of "making data public" has a narrow meaning under the Turkish Data Protection Act, and only covers scenarios where the data subjects wish the data to be public for data processing – the mere act of making personal data available to the public is not sufficient.

- On 26 October 2020, the KVKK issued a statement on cross-border data transfers outside of Turkey.[90] The statement noted that the Turkish Data Protection Act allowed a grace period for compliance with relevant data transfer provisions, and that several deadlines had been extended due to the COVID-19 pandemic. The KVKK also committed to eliminate and correct any misunderstandings arising from the interpretation and implementation of the Act, which had led to criticism from practitioners and scholars. As a start, the KVKK clarified that the Board will carry out assessments on the adequacy of foreign jurisdictions for data transfers based on a number of factors, including the reciprocity concerning data transfers between the importing country and Turkey. The KVKK also indicated that "Binding Corporate Rules" ("BCRs") may be applicable and used in data transfers between multinational group companies. Indeed, on 10 April 2020, the KVKK introduced BCRs to the Turkish data protection law, to be used in cross-border personal data transfers of multinational group companies.[91] In its announcement, the KVKK described the undertaking letter procedure for data transfers outside of Turkey, and states that although the undertaking letters make bilateral data transfers easier; they may be inadequate in terms of data transfers between multinational group companies. Therefore, the KVKK determined BCRs as another mean that could be used in international data transfers between group companies.

- On 17 July 2020, the KVKK issued a statement on de-indexing of personal data from search engine results[92] based on the Board's decision with number 2020/481.[93] The KVKK stated in its announcement that, they have evaluated the applications submitted before the KVKK with regards to the requests as to de-indexing web search results and within the scope of "right to be forgotten", the Board decided that search engines should be considered as "data controllers" under the Turkish Data Protection Act, that individuals may primarily convey their de-indexing requests to the search engines and file complaints before the KVKK and search engines should make a balance test between fundamental right and freedoms and public interest. Additionally, KVKK also published a criteria document[94] by indicating that de-indexing requests should be considered per the issues indicated therein, which is mainly based on Article 29 Working Party's Opinion on the Guidelines on the Implementation of the Court of Justice of the European Union Judgment on Costeja Case.

- On 26 June 2020, the KVKK issued a statement on obligation to inform data subjects.[95] The statement concerns the general rules that are already regulated under the Turkish Data Protection Act and secondary legislation concerning the obligation to inform set forth for the data controllers. KVKK indicated in its announcement that privacy policies or data processing

policies should not be used to fulfill the obligation to inform and thus, privacy notices should be separated from these texts. Following that, the KVKK listed several examples with regards to the deficiencies and illegalities as to obligation to inform.

- In the context of the COVID-19 pandemic, on 9 April 2020, the KVKK issued a statement on the processing of location data in light of the COVID-19 pandemic.[96] The statement highlights that many other countries have used and allowed the use of personal data, such as the health, location and contact information of individuals, to identify those who carry or are at risk of carrying this disease. The KVKK reminds that the processing of this data needs to be carried out within the framework of the basic principles enshrined in the Turkish Data Protection Act.

2. Turkish Data Protection Act Continues to be Enforced

2020 was also a year in which the KVKK enforced the Turkish Data Protection Act in a number of data protection proceedings.

On 6 February 2020, the KVKK fined an undisclosed bank TRY 210,000 (approx. €27,800) for illegally processing personal data to gain potential customers.[97] The case concerned the creation of bank accounts without the knowledge or consent of individuals, using information gained by the bank via a third party. The KVKK found that the bank had acted in breach of its security obligations to prevent unlawful processing of personal data.

On 22 July 2020, the KVKK fined an automotive company TRY 900,000 (approx. €101,840) for violations related to the transfer of personal data based on the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data ("**Convention 108**").[98] The software provider sought to rely on the fact that the receiving country was party to Convention 108 and, therefore, offered sufficient protection to personal data imported from Turkey. However, the KVKK outlined that the fact that a receiving country is a party to Convention 108 is in itself an insufficient measure in determining adequate protection of data. The data transfer had thus been carried out in breach of the Turkish Data Protection Act, without data subjects' consent and not benefitting from any of the exceptions set out in the Turkish Data Protection Act. It is worth noting, in this regard, that the KVKK is yet to publish the list of countries deemed to provide sufficient protection under Turkish law. Finally, the decision notes that the data controller failed to comply with its data security obligations, as it had failed to prevent the unlawful processing and transfer of personal data. The KVKK ordered the data controller to delete/destroy the personal data unlawfully transferred outside of Turkey.

On 16 April 2020, the KVKK fined a gaming company TRY 1,100,000 (approx. €120,000) for failing to notify the KVKK of data breach within seventy-two (72) hours after becoming aware of the relevant data breach and to take required data security measures.[99]

On 27 February 2020, the KVKK fined an e-commerce company TRY 1,200,000 (approx. €120,000) mainly, TRY 1,100,000 for failing to fulfil the obligations relating to data security and TRY 100, 000 for failing to comply with the obligation to inform data subjects.[100] Besides, the Board also ordered the data controller to revise the data processing processes and privacy policy, Conditions of Sale and Use and Cookie Notice in accordance with the determined irregularities and in line with the Turkish

Data Protection Act. The Board stated in its decision that (i) the privacy policy contains lots of information and general information about personal data processing and this does not mean that the data subjects are duly informed; (ii) although the data processing activities start with the cookies as soon as a user enters the website, information obligation is not complied with at any stages such as cookies or member login to the website; (iii) explicit consent is not obtained for commercial electronic communications and cross-border transfer of personal data; and (iv) considering that the undertaking letters submitted for cross-border transfer of personal data are not approved and the safe countries have not been announced, data controller may only transfer personal data abroad based on data subjects' explicit consent.

III. Developments in Asia-Pacific, Middle East and Africa

A. Australia

The Australian government released the Terms of Reference and Issues Paper for the review of the Privacy Act 1988, and solicited public submissions by 29 November 2020. This wholesale review may update main provisions of the Privacy Act 1988, such as increasing maximum civil penalties, creating a binding privacy code for social media platforms, strengthening notification and consent requirements, modifying international data transfers, and expanding the definition of personal information. The government plans to issue a discussion paper seeking specific feedback on preliminary outcomes and possible areas of reform in early 2021.

B. China

1. New Developments in Chinese Legislation

The most significant legislative framework in China for the protection of personal data is the Cybersecurity Law ("**Cybersecurity Law**") which came into effect on 1 June 2017. Two additional laws were introduced into the pipeline in 2020: the Draft Personal Information Protection Law[101] ("**Draft PIPL**"); and the Draft Data Security Law ("**Draft DSL**"). Once adopted, the combination of these three legal instruments (the Cybersecurity Law, the Draft Data Security Law and the Draft PIPL) are expected to become the fundamental laws in the field of cybersecurity and data protection in China.

The **Draft PIPL** is intended to be a general data protection law, which could harmonise the current fragmented legislative framework. However, even after the adoption of the Draft PIPL, personal information protection in China would remain sector based.

The Draft PIPL was partially inspired by the GDPR, but it has important differences that prevent a common cross-border approach (*e.g.*, regarding the legal grounds for data processing, there is no legal basis of legitimate interest of the controller). Using a single privacy framework for EU and Chinese companies would consequently not result in adequate compliance.

The Draft PIPL introduces substantial new fines. For example, data processors are subject to fines of RMB 50 million (approx. €8 million, or $7.4 million), or 5% of the company's revenue from the previous

year.[102] In addition, the Cyberspace Administration of China would also have the competence to blacklist organisations and individuals for misusing data subjects' data.[103]

On 18 November 2020, the Centre for Information Policy Leadership ("**CIPL**") submitted recommendations on possible modifications of the Draft PIPL in order to ensure the protection of China's citizens, businesses and government data,[104] including the following:

- The Draft PIPL includes definitions for sensitive personal information,[105] including biometric, financial, ethnic and religious information. The CIPL suggested a risk-based approach to assess personal data processing, rather than providing categories of predefined "sensitive information".
- According to the CIPL, exemptions should be provided to the general requirement to appoint data protection officers and representatives, in line with other foreign privacy laws like the GDPR.
- The Draft PIPL should explain further what conditions or factors are required to satisfy the Cyberspace Administration's security assessment for cross-border transfers of personal data.
- The Draft PIPL should clarify what constitutes a "serious" unlawful act.
- Finally, the CIPL recommended that organisations be afforded a two-year grace period from the date that the Draft PIPL is passed, to be fully compliant.

The other major legislative proposal, the **Draft DSL**, is intended to provide the fundamental rules of data security for both personal and non-personal data. The intended scope of application of the Draft DSL is broad, applying to "activities" (actions including collection, storage, processing, use, supply, trade and publishing) regarding "data" (any record of information in electronic or non-electronic form).

Finally, on 1 January 2021 the Civil Code of the People's Republic of China entered into force, adopted by the third session of the 13th NPC. The Civil Code applies to all businesses in general (without distinguishing among controllers and processors), and introduces rules for the protection of personal information, including its collection, use, disclosure, and processing.

2. Enforcement of Chinese Data Protection and Cybersecurity Legislation

In August 2020, the China Banking and Insurance Regulatory Commission ("**CBIRC**") issued two separate fines of RMB 1 million ($150,000) on two banks.[106] In both cases the banks were fined for failures to provide protection to personal data of credit card customers.

C. Hong Kong SAR

On June 30, 2020, the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region (the "**NSL**") passed by the Standing Committee of the National People's Congress of the People's Republic of China (the "**PRC**") became effective in Hong Kong. The NSL empowers law enforcement authorities to search electronic devices and premises that

may contain evidence of related offenses and carry out covert surveillance upon approval of the Chief Executive; criminalizes acts of terrorism, subversion, secession, or collusion with foreign or external forces to endanger national security; and holds incorporated or unincorporated entities accountable for violations of the NSL.

Furthermore, the Committee for Safeguarding National Security (the "**Committee**"), which consists of specified Hong Kong officials and an advisor appointed by the Central People's Government of the PRC (the "**CPR**"), is established pursuant to the NSL and assumes various duties including formulating work plans and policies, advancing the enforcement mechanisms and coordinating significant operations for safeguarding national security in Hong Kong. Decisions made by the Committee are not subject to judicial review.

The Office for Safeguarding National Security of the CPG (the "**Office**") may in specified circumstances assume jurisdiction over serious or complex cases which would be difficult or ineffective for Hong Kong to handle in light of, for example, involvement of a foreign country or external elements. Such cases shall be investigated by the Office and, upon prosecution by a body designated by the Supreme People's Procuratorate, adjudicated by a court designated by the Supreme People's Court of the PRC.

The NSL applies not only to offenses committed or having consequences in Hong Kong by any person or entity, but also offenses committed from outside Hong Kong against Hong Kong by any person or entity.

D. India

1. Legislative initiatives

As indicated in the 2020 International Outlook and Review, the Personal Data Protection Bill 2019 ("**PDP Bill**") was introduced in Parliament on 11 December 2019 adapted from the draft data protection legislation presented to the Ministry of Electronics and Information Technology on 27 July 2018[107], by the committee of experts led by Justice Srikrishna. Thereafter the PDP Bill was referred to a Joint Parliamentary Committee for its review. As of January 2021, the PDP Bill is in its final stages of deliberation and is expected to be promulgated soon. Several industry bodies and stakeholders were asked to depose before the Joint Parliamentary Committee for their views on the amendments made in the PDP Bill and the desired requisites of a national data protection law. 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.

In September 2019, the Ministry of Electronics and Information Technology constituted a committee of experts ("**Committee**") to devise a framework for the regulation of non-personal data. Ultimately, on 12 July 2020, the Committee released a Report on Non-Personal Data Governance Framework ("**NPD Framework**")[108], where it emphasised that the regulation of non-personal data is necessary to incentivise innovation, create value from data sharing, address privacy concerns, and prevent harm. The NPD Framework was met with criticism for the imposition of compulsory data sharing obligations and onerous compliance requirements on entities collecting and managing non-personal data. After reviewing feedback from public and stakeholders, the Committee released a revised version of the NPD

Framework on 1 January 2021, wherein the Committee provided several clarifications to the earlier draft and streamlined the jurisdictions of the PDP Bill and the NPD Framework. The NPD Framework is still under public consultation and is yet to be presented before the Parliament as a bill for the promulgation of a single national-level regulation to establish rights over non-personal data collected and created in India.

In August 2020, the Government of India also proposed a data-sharing framework in the fintech sector. The National Institution for Transforming India ("**NITI Aayog**") released a draft framework on the Data Empowerment and Protection Architecture[109] which will be implemented by the four government regulators: the Reserve Bank of India, the Securities and Exchange Board of India, the Insurance Regulatory and Development Authority, and the Pension Fund Regulatory and Development Authority, and the Ministry of Finance. The draft aims to institute a mechanism for secure consent-based data sharing in the fintech sector, which may be an important step towards empowering individuals in relation to their personal data. The draft aims to enable individuals to share their financial data across banks, insurers, lenders, mutual fund houses, investors, tax collectors, and pension funds in a secure manner.

In August 2020, the Government of India also launched the National Digital Health Mission ("**NDHM**"), a visionary project which intends to digitise the entire health care ecosystem of India. The National Health Data Management Policy, 2020[110] came into force on 15 December, 2020, and is the first step in realising the NDHM's guiding principle of "*security and privacy by design*" for the protection of data principals' personal digital health data privacy. It is intended to be a guidance document across the National Digital Health Ecosystem and sets out the minimum standard for data privacy protection for data relating to the physiological and psychological health of individuals in India.

2. Regulatory opinions and guidance

Indian institutions have also adopted certain measures in response to the challenges resulting from the COVID-19 pandemic. For instance, the Data Security Council of India ("**DSCI**") issued the best practices on working from home in light of COVID-19[111] on 18 March, 2020. The guidance notes, among other things, that virtual private networks should only be used on company-owned devices, employees should access company data and applications through a browser-based webpage or virtual desktop, and a risk assessment should be conducted when selecting a remote access method. In addition, the guidance outlines a basic mandate for organisations and employees, which includes taking care of the confidentiality of valuable transactions and sensitive financial documents when working from home.

In a similar vein, the DSCI published, on 24 April 2020, its guidelines on data privacy during the COVID-19 pandemic, which highlights the privacy implications of COVID-19 for different sets of stakeholders and provides privacy and data protection practices.[112] The guidelines address healthcare privacy considerations and note the importance of notifying patients of all information that is collected, having specific protocols in place to ensure that consent is obtained, having internal and external audit mechanisms to assess privacy measures, and using health data solely for the specific purposes of their collection. Finally, the guidelines provide working from home considerations both for employers and employees, noting the importance of revisiting data protection strategies, data management practices,

remaining compliant with regulatory obligations, conducting Data Protection Impact Assessments to ascertain privacy risks, and spreading privacy awareness and training across organisations.[113]

The DSCI also published its Report for Enabling Accountable Data Transfers from India to the United States Under India's Proposed Personal Data Protection Bill on 8 September 2020[114] ("**Report on Data Transfers**"). The purpose of the Report on Data Transfers is to make additional recommendations to the existing draft of the PDP Bill to enable free flow of data between countries, especially with the U.S. owing to the value it adds to India's digital economy, and to provide solutions for facilitating India-US data transfers. The Report on Data Transfers also suggests, among other things, that the PDP Bill's provision on the creation of codes of practice should include certification requirements in order to increase interoperability between different privacy regimes as well as facilitate cross-border transfer mechanisms.

On 2 September 2020, the Artificial Intelligence Standardisation Committee for the Department of Telecommunication released its Indian AI Stack discussion paper.[115] The Discussion Paper notes that the AI Stack will, among other things, secure storage environments that simplify archiving and extraction from data based on the data classification, ensure the protection of data through data federation, data minimisation, an open algorithm framework, defined data structures, interfaces and protocols, and monitoring, auditing, and logging, as well as ensuring the legitimacy of backend services.

3. Enforcement of data protection laws

In 2020, the Government of India adopted three decisions to block applications following information that they were engaging in activities which were prejudicial to the integrity and the national security of India.[116]

In particular, the Government had received complaints regarding the misuse of mobile application data, stealing and secretly transmitting users' data in an unauthorised manner to servers located outside of India. As a result, on 29 June 2020, the Government decided to disallow the use of 59 applications to safeguard the interests of Indian mobile and internet users.[117] Similarly, on 2 September 2020[118], and 29 November, 2020,[119] the Indian Government decided to further block 118 and 43 mobile applications respectively for misusing users' data and engaging in activities which are prejudicial to the sovereignty, integrity and defence of India, as well as the security of the state and public order. According to the Government, the applications' practices raised concerns relating to the fact that they were collecting and sharing data in a manner which compromised the personal data of users, posing a severe threat to the security of the State.

On 23 November 2020, the Orissa High Court delivered an important judgment emphasising the need to recognise the right to be forgotten, noting the presence of objectionable images and videos of rape victims on social media platforms.[120] The court emphasised that the principle of purpose limitation is already embodied in law by virtue of the precedent of the Supreme Court's judgment in *K.S. Puttaswamy v. Union of India*, and that capturing images and videos with the consent of the victim cannot justify the subsequent misuse of such content. The court referred to existing case law and the PDP Bill, which provide for the right to be forgotten. Accordingly, the court recognised the right to be forgotten

as a right *in rem* and stressed that, in the absence of legislation, victims may nevertheless seek appropriate orders to have offensive posts erased from public platforms to ensure protection their right to privacy.

E. Indonesia

On 24 January 2020, a draft of the Personal Data Protection Act ("**PDP Bill**") was submitted to the Indonesian House of Representatives.[121] 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.[122]

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.[123] However, it appears that the COVID-19 pandemic has led to delays in the adoption of the Bill.

Finally, on 10 March 2020, Kominfo submitted a new draft regulation on the Management of Privately Managed Electronic System Organiser ("**Draft Regulation**") for approval. The Draft Regulation is intended to serve as an implementing regulation of Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions, which, as noted in the 2020 International Outlook and Review, became effective in October 2019.

F. Israel

On 29 November 2020, the Israeli Ministry of Justice ("**MoJ**") launched a public consultation on the introduction of amendments to the Protection of Privacy Law 5741-1981.[124] The MoJ also launched, on 23 July 2020, a public consultation on proposed amendments to privacy law database registration requirements which would reduce the scope of the obligation to register a database and amend certain definitions contained in the law.[125]

Moreover, the Privacy Protection Authority ("**PPA**") published a number of reports and recommendations on a series of topics, including:

- privacy protection in the context of epidemiological investigations,
- security recommendations following security incidents,
- the protection of privacy in the context of money transfers and app payments,
- data processing and storage service providers,
- smart transportation services,
- digital monitoring tools for COVID-19 contact tracing,
- GSS assistance in contact tracing,

- recommendations in the context of the COVID-19 pandemic (*e.g.*, remote learning, privacy for individuals entering workplaces, medical institutions privacy compliance).

Following the CJEU's decision to annul the EU-U.S. Privacy Shield in *Schrems II*, the PPA issued, on 29 September 2020, a statement regarding transfers of personal information from Israel to the U.S. In this statement, the PPA indicated that data transfers from Israel to the U.S. could no longer rely on the EU-U.S. Privacy Shield or the Transfer of Information Regulations, and that alternative exceptions provided for in Section 2 of the Regulations could only be used where applicable. The PPA had nonetheless clarified that personal data could be transferred from Israel to EU Member States, as well as to countries which will cease to be EU Member States but will continue to apply and enforce the provisions of EU Law on the protection of personal data.[126]

On the enforcement side, in 2020 the PPA identified and investigated a number of violations, including the leak of personal data of 6.5 million Israeli voters.[127] The PPA also offered security recommendations following the security incident at an insurance company.

G. Japan

On 5 June 2020, the Parliament of Japan adopted a bill to amend the currently applicable general data protection law, the Act on the Protection of Personal Information ("**APPI**").[128]

Under the bill, the rights of the data subjects have been expanded. For example, if the proposed amendments to the APPI are introduced, data subjects will be entitled to request an organisation to delete their personal information, but only if certain requirements are met. Consequently, the scope has remained narrower than the right to erasure and the right to object under the GDPR.

Regarding data retention periods, the currently applicable law provides that any data which was to be erased after six months is not considered as "retained personal data", and therefore is not not subject to data subject requests. The Amendments will abolish this six-month rule, and data subjects will be able to exercise their data-related rights regardless of the retention period.

Under the current applicable law, organisations should "duly make an effort" to report data breaches to the Personal Information Commission ("**PIC**"). In contrast, the bill will introduce a mandatory obligation to notify data breaches, obliging organisations to report data breaches to the PIC and to notify the affected data subjects if their rights and interests are infringed. Although this requirement is similar to the corresponding provisions in the GDPR, the latter sets a strict deadline of 72 hours for notification, while the bill requires "prompt" reporting.

The amended APPI will include the concept of "pseudonymously processed information", which similarly to the GDPR will mean personal information that cannot be used to identify an individual unless combined with other information. Pseudonymously processed information will not be subject to some requirements, such as requests for disclosure, utilisation, or correction. In the event of a data breach concerning pseudonymously processed information, reporting to the PIC will not be mandatory.

One of the main goals of the bill is to address the increasing risks associated with cross-border data transfers. Under the new provisions, data subjects should be informed about the details of any data transfer to a third party located in a foreign country. The bill has also increased the criminal penalties, such as the penalty for violating an order of the PIC (100 million yen; approx. €800,000). However, administrative fines will not be introduced.

The bill is expected to enter into force no later than June 2022. The new rules will bring the APPI into closer alignment with the EU's data protection standards and strengthen Japan's data protection regime.

H. Malaysia

On the legislative side, on 14 February 2020, a public consultation paper was released proposing amendments to the Malaysian Personal Data Protection Act 2010, which currently regulates data protection in Malaysia.[129] If adopted, the amendments would introduce significant changes to Malaysia's data protection regime, including: the obligatory appointment of a data protection officer, mandatory breach reporting, the introduction of civil litigation against data users, the implementation of technical and organisational measures such as data portability and privacy by design, and the broadening of the Malaysian Personal Data Protection Act's scope to data processors. Many of the proposed amendments have been inspired by the GDPR and aim to bring the Malaysian regime closer to EU data protection standards.

On 29 May 2020, the Department of Personal Data Protection ("**PDP**") released advisory guidelines on the handling of personal data by businesses under the Conditional Movement Control Order.[130] The advisory guidelines highlight that only names, contact numbers, and the dates and times of attendance can be collected from customers, and requires a clearly visible notice detailing the purpose of collection. The PDP also advises that personal data should only be collected for informational purposes and must be permanently deleted six months after the Control Order is terminated.

I. Singapore

As explained in the 2020 International Outlook and Review, Data protection in Singapore is currently governed by the Personal Data Protection Act 2012 ("**Singapore PDPA**").

The Personal Data Protection Commission ("**PDPC**") conducted a review of the Singapore PDPA and, on 14 May 2020, the PDPC released a joint statement with the Ministry of Communications and Information announcing the launch of an online public consultation on a bill to amend the Singapore PDPA and the Spam Control Act 2007 ("**SCA**").[131]

On the basis of this, the proposed amendments to the Singapore PDPA to address Singapore's evolving digital economy needs, and related amendments to the SCA, were passed in Parliament on 2 November 2020.[132] The bill introduced several notable amendments, including mandatory data breach notification requirements, enabling meaningful consent where necessary and providing consumers with greater autonomy over their personal data through the incorporation of a data portability obligation.[133] Moreover, the bill strengthened the enforcement powers of the PDPC.[134]

Subsequently, on 20 November 2020, the PDPC issued the draft Advisory Guidelines on Key Provisions of the Personal Data Protection (Amendment) Bill ("**Draft Advisory Guidelines**").[135] The Draft Advisory Guidelines provide clarifications on key provisions in the bill, covering, *inter alia*, the framework for the collection, use, and disclosure of personal data, mandatory breach notification requirements, financial penalties, and offences for mishandling personal data. The Draft Advisory Guidelines will be finalised and published when the amendments to the Singapore PDPA come into effect, *i.e.*, upon their signing and publication in the Gazette, which is expected in early 2021.

J. South Korea

In January 2020, the National Assembly of the Republic of Korea adopted amendments ("**Data 3 Act**") to the Personal Information Protection Act 2011 ("**PIPA**")[136] and to other main data protection laws. The adoption of the Data 3 Act meant the implementation of a more streamlined approach to personal data protection in South Korea. In addition, it is expected that these legislative changes will facilitate the adequacy assessment under the GDPR and the adoption of an adequacy decision from the European Commission.

The Data 3 Act aims to extend the powers of the Personal Information Protection Commission ("**PIPC**"), which will be the supervisory authority for any data breaches. Data protection issues are currently handled by several different agencies, but with the entry into force of the reforms these will now be handled exclusively by the PIPC. In addition, the PIPC will have the competence to impose fines similar to those provided under the GDPR.

The Data 3 Act introduced to the PIPA the concept of "pseudonymised information" (*i.e.*, personal information processed in a manner that cannot be used to identify an individual unless combined with other information). Pseudonymised information may be processed without the consent of the data subject for purposes of statistical compilation, scientific research, and record preservation for the public interest.

Finally, it should be noted that the cross-border transfer of the personal data of Korean data subjects has remained restricted as their consent is required prior to transferring their personal data abroad.

K. Thailand

As noted in the 2020 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, the government of Thailand approved a Royal Decree to postpone the application of the Thailand PDPA until 31 May 2021, citing the negative effects of the COVID-19 pandemic as one of the main reasons for doing so.[137]

Subsequently, on 8 June 2020, the Ministry of Digital Economy and Society ("**MDES**") issued a statement on the Thailand PDPA's postponement, noting that government agencies, and private and public institutions, were not ready for the enforcement of the legislation.[138] This was followed by a notice published by the MDES on 17 July 2020 for data controller requirements and security measures to be implemented during the postponement period of the Thailand PDPA.[139]

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 the 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 by 27 May 2021.

L. United Arab Emirates

On 19 November 2020, the Abu Dhabi Global Market ("**ADGM**")[140] announced the issuance of a public consultation on proposed new Data Protection Regulations 2020 amending the existing Data Protection Regulations 2015.[141] The proposed draft aims at aligning the ADGM with certain international standards, especially the GDPR,[142] and introduces, amongst other things, the following elements: definitions, the principles of accountability and transparency, the processing of special categories of data, individual rights, security obligations, and the notification of data breaches. The proposed data protection framework is aimed to have a broad scope of application, including the processing of personal data in the context of the activities of an establishment in ADGM, regardless of whether the processing takes place in ADGM. In a similar vein, it will apply to natural persons, whatever their nationality or place of residence, excluding cases where a data controller is only connected to ADGM because it uses a data processor located inside the ADGM. In the latter case, the Proposed Data Protection Framework would not apply to the data controller.[143]

On 1 July 2020, the Dubai International Financial Centre (the "**DIFC**") published the Data Protection Regulations, which entered into effect on the same date with the Data Protection Law No. 5 of 2020.[144] In particular, the Regulations comprise provisions regarding, in particular, the content and format to be followed by personal data processing records, activities requiring data processing notifications to the Data Protection Commissioner, conditions to transfer data outside of the DIFC, and fines. Moreover, in September 2020, the DIFC became a fully accredited member of the Global Privacy Assembly ("**GPA**").[145]

M. Other Developments in Africa

Data protection authorities in Africa have generally been monitoring compliance with data protection requirements, especially in the context of the COVID-19 pandemic. Moreover, Nigeria and other African nations have developed a framework that aims to harmonise laws on data protection and the digital economy.[146]

Egypt: On 17 July 2020, Resolution No. 151 of 2020 ("**Egypt Data Protection Law**") was approved and published in the official gazette, and within three months it came into force.[147] The Egypt Data Protection Law governs the processing of personal data carried out electronically, in part or in full, and gives to data subjects' rights in relation to the processing of personal data. The key elements that the law provides for are the following:

- consent is the main legal basis for the processing of personal data;

- conditions and principles for data processing must be respected;
- the Centre for the Protection of Personal Data is the regulatory body aiming to maintain compliance with the Egypt Data Protection Law; and
- activities covered include the processing of sensitive personal data, cross-border transfers, electronic direct marketing practices, monetary penalties and criminal sanctions for violations of the Egypt Data Protection Law itself.

Kenya:[148] The Information Technology Industry Council ("**ITI**") announced, on 28 April 2020, that it had submitted comments to the Office of the U.S. Trade Representative on the U.S. and Republic of Kenya Trade Agreement negotiations. These comments include measures that should ensure protection of personal data by taking into account best international practices for privacy and interoperability, strengthen regulatory practices in emerging technologies such as artificial intelligence and machine learning, and promote risk-based cybersecurity and vulnerability disclosure in alignment with international standards.[149] The formal negotiations were launched in July 2020.[150]

Namibia: Namibia has not yet enacted a comprehensive data protection legislation. On 24 February 2020, the Council of Europe organised, in coordination with Namibia's Ministry of Information and Communication Technology, a two-day stakeholders' consultation workshop on a draft data protection bill for Namibia.[151] A draft of the bill is expected to be published in 2021.

Nigeria: In Nigeria, data privacy is currently protected by a comprehensive data protection regime comprising a variety of laws, regulations, and guidelines. As underlined in a statement, issued on 27 January 2020 by the National Information Technology Development Agency ("**NITDA**"), the Nigeria Data Protection Regulation concerns the use, collection, storage or transfer of personal data and intends to provide a clear framework for data protection in Nigeria. However, pursuant to the Nigerian Communications Commission, appropriate legal instruments must be put in place in order in order to strengthen cybersecurity.[152]

The NITDA issued, on 17 May 2020, its Guidelines for Management of Personal Data by Public Institutions in Nigeria.[153] On 20 August 2020, the NITDA had published the Draft Data Protection Bill 2020 for public comments. The Draft Bill aims primarily to promote a code of practice that ensures the protection of personal data and its lawful, fair and transparent process in accordance with the principles set out in the Draft Bill while taking into account the legitimate interests of commercial organisations as well as government security agencies. In addition, the Draft Bill provides for a Data Protection Commissioner, an impartial, independent and effective regulatory authority.

South Africa:[154] In 2013, the Protection of Personal Information Act ("**POPIA**") was signed into law by the President of South Africa and the Information Regulator was established as the supervisory authority. In June 2020, the President announced that certain essential remaining sections of POPIA would commence to apply on 1 July 2020 and that, following a 12-month transition period, public and private bodies would need to comply from 30 June 2021.

In addition, on 3 April 2020, the South African Regulator published a guidance note on processing personal information during the Coronavirus pandemic encouraging proactive compliance by responsible parties when processing personal information belonging to COVID-19 cases and their contacts.[155]

Togo: On 9 December 2020, the National Assembly announced that it had adopted a draft decree on the organisation and functioning of the body for the protection of personal data, the IPDCP, which will have a power of investigation and enforcement in order to support the government's policy on personal data protection.[156]

Rwanda: A final draft of the data protection bill was approved and published on 27 October 2020 by the Office of the Prime Minister of the Republic of Rwanda.[157] The Bill includes provisions on data subject rights, general rules for data collection and processing, and procedures for data activities, such as transfers, sharing and retention.[158] Moreover, the Ministry of ICT and Innovation (MINICT) published, on 5 May 2020, COVID-19 guidelines addressing cybersecurity measures.[159]

N. Other Developments in the Middle East

Whereas data protection was mainly provided for in sectoral regulations, privacy laws are progressively emerging across the region.

Oman: On 12 July 2020, the State Council of the Sultanate of Oman announced that it had held discussions on the draft law on the protection of personal data, which comprises in particular provisions regarding the role of the Ministry of Technology and Communications, the responsibility to protect the rights of personal data owners, and the obligations of controllers and processors, as well as the applicable sanctions.[160] The State Council also announced on 10 September 2020 that it had discussed a draft law of a new legislation dealing with cybersecurity. The Technology and Innovation Committee of the State Council had approved in part the content of the draft law.

Pakistan: Data protection is still governed through sectoral legislation. However, the Ministry of Information Technology and Telecommunication ("**MOITT**") finalised the draft Personal Data Protection Bill 2020 which was presented to the Cabinet of Pakistan for approval.[161] The bill, which was introduced in April 2020, provides for the general requirements for personal data collection and processing and contains several similar provisions to those found within GDPR, but is silent regarding the right to data portability and does not require data controllers to notify data subjects of data breaches. In addition, the MOITT adopted, on 18 November 2020, social media rules setting measures and obligations applicable to social media and internet providers in order to prevent unlawful online content and to protect national security.[162]

O. Other Developments in Southeast Asia

Throughout 2020, developments related to the data protection and cybersecurity landscape occurred in certain other jurisdictions in the south-eastern subregion of Asia, including the following:

Cambodia: While the country does not have a general personal data protection law or a data protection authority, there have been recent legislative developments addressing relevant areas. In particular, a draft cybercrime law is currently being prepared that would regulate Cambodia's cyberspace and security, aiming to prevent and combat cyber-related crimes.

Philippines: On 9 March 2020, the APEC Cross-Border Privacy Rules ("**CBPR**") system Joint Oversight Panel approved the Philippines' application to join the APEC CBPR system. As such, the Philippines becomes the ninth APEC economy to join the CBPR system.

The institutions in the Philippines have been particularly active in formulating data protection measures and statements to address issues relating to the collection and processing of data in the wake of the COVID-19 pandemic. On 1 June 2020, the Philippines created a task force in order to drive practical responses to privacy issues emerging from the pandemic.

Vietnam: The data protection framework in Vietnam was fragmented, and relevant provisions can be found in numerous laws. In 2020, the government of Vietnam issued Decree No. 15/2020/ND-CP, providing for regulations on penalties for administrative offences in the sectors of post, telecommunication, radio frequency, information technology, and electronic transactions, which is in effect as of 15 April 2020. In February 2020, however, a draft personal data protection decree was released, which has already undergone public consultation. The draft decree 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 decree contains provisions on obtaining consent of data subjects, the technical measures needed to protect personal data, and the creation of a data protection authority.

IV. Developments in Latin America and in the Caribbean Area

A. Brazil

The biggest data protection development in Brazil in 2020 was the entry into force of Law No. 13.709 of 14 August 2018, the General Personal Data Protection Law[163] (as amended by Law No. 13.853[164] of 8 July 2019) ("**LGPD**") on 18 September 2020. The specific enforcement provisions of the LGPD are expected to enter into force on 1 August 2021, further to an additional law passed in June 2020.

Compared to the EU's GDPR, the LGPD shows both differences and similarities. The definitions of "personal data" are very similar in both instruments, both having the goal of assuring a high level of protection for any "*information related to an identified or identifiable natural person*". Thus, anonymised data falls expressly out of scope in the two jurisdictions, with a caveat on the Brazilian side existing in the sense that if anonymised data is used to create or enhance the behavioural profiling of a natural person, it may also be deemed as personal data, provided that the impacted person can be identified in the process.

Both legislations apply to the processing of personal data carried out by both public and private entities, online and offline. As for the territorial scope, the rules apply to organisations that are physically present

in the EU and Brazil as well as to organisations that, although not located in those states/regions, may offer goods or services there. When it comes to the handling of sensitive data, the LGPD sets forth a narrower list of legal grounds that can be elected to legitimise the processing of such data, such as the necessity to comply with a legal obligation, to protect the life and physical safety of the subject or a third party, for the exercise of rights in contractual or judicial proceedings and for the prevention of fraud.

The LGPD offers ten legal grounds for processing of personal data, which are comparable to the ones provided in the GDPR. In addition, the LGPD offers four additional grounds that may authorise the processing of personal data, namely for the conduction of studies of research bodies, for the exercise of rights in judicial, administrative, and arbitral proceedings, for the protection of health in procedures conducted by health professionals and health entities, and for the protection of credit.

Both the LGPD and the GDPR expressly provide for a set of rights granted to data subjects with respect to their personal data. Both norms recognise individuals' right of access to their personal data, right to be informed of processing activities based on their personal data, and rights of rectification and erasure. Although the rights prescribed in both pieces of legislation are fairly similar, it could be argued that the major element that sets both norms apart are the timeframes for responding to data subject requests. While on the European side organisations must generally respond to requests within one month of the receipt of a request, the LGPD is limited to a 15-day period for complying with access requests, while requests for the exercise of other rights should be responded to immediately.

The role of data protection officers ("**DPOs**") is fairly similar under both legislations. DPOs are legally tasked with acting as a point of contact between the organisation they represent, the supervisory authorities, and data subjects, as well as advising and orienting the organisation they represent with regard to its data protection obligations. There are, however, two major differences between the Brazilian and the EU rules concerning the position of DPOs. The first one is that the GDPR expressly specifies instances where an organisation is required to appoint a DPO, while the LGPD makes no such limitation, thus obliging virtually every organisation subject to its scope to appoint one. The second difference is that, while the GDPR establishes the need for DPOs to be independent within the organisational structure of their organisations and also to be provided with monetary and human resources to fulfil their tasks, the LGPD does not provide such express guidance.

A significant difference between the two instruments is their enforcement. The legal structure of the Brazilian supervisory authority lacks some traits of independence and autonomy when compared to the structure provided for under the GDPR. However, the LGPD has introduced a number of sanctions that can be imposed by the ANPD, such as public disclosure of a violation, erasure of personal data relating to a violation, and even a temporary suspension of data processing activities. The entry into force of the provisions of the LGPD governing administrative sanctions has been deferred to 1 August 2021.

On 23 September 2020, Bill 4695/2020,[165] seeking to protect the personal information of students when using distance learning platforms, was introduced. The bill would require distance learning platforms to follow data processing requirements provided by the LGPD and to, whenever possible, use the technology without collecting and sharing personal and sensitive data, revealing racial origin,

religious or political beliefs, or genetics of the users. Furthermore, the bill requires that processing of personal data can only take place when prior and express consent has been obtained.

Finally, on 18 December 2020, the National Telecommunications Agency ("**Anatel**") approved the Cybersecurity Regulation[166] applied to the telecommunications sector. The regulation is intended to promote cybersecurity in telecommunications networks and services and support ongoing supervision of the market, infrastructures, and the adoption of proportional corrective measures. Moreover, the regulation imposes an obligation on telecommunication providers to develop, maintain and implement a detailed cybersecurity policy, which must include, *inter alia*, national and international norms, best practices, risk mapping, incident response time and sharing and sending information to Anatel. The regulation came into force on 4 January 2021.

B. Other Developments in South America

1. Argentina

On 28 January 2020, The Argentinian data protection authority ("**AAIP**") issued a resolution[167] against a telecommunication company for violations of Law No. 26.951 ("**DNC Law**").[168] In particular, the AAIP issued a fine of ARS 3,000,000 (approx. €45,000) for 248 charges relating to violations of Article 7 of the DNC Law, which provides that those who advertise, offer, sell or give away goods or services by means of telephone communications may not address any individual who is registered in the "Do Not Call" registry.

On 6 June 2020, the AAIP imposed a fine[169] of ARS 280,000 (approx. €3,770) against a tech company for violations of the Personal Data Protection Act No. 25.326 of 2000. In particular, the AAIP found that the company did not allow a user to access their personal data in their email account and related applications after changes to their passwords were made by an un-authorised third party.

2. Chile

On 1 June 2020, the Chilean Transparency Council ("**CPLT**") announced that an audit of 12,000 purchase orders made by 86 organisations in the health sector had revealed some disclosures of sensitive personal data of patients without their express consent.[170] Moreover, the CPLT highlighted that in some cases the data had even been made public through online platforms. To remedy that, the CPLT has offered technical support to the Chilean Ministry of Health.[171]

3. Colombia

On 26 November 2020, the Colombian data protection authority ("**SIC**") announced that it had issued an order[172] requiring a videoconference service provider (with no physical presence in Colombia) to implement new measures guaranteeing the security of personal data of its users in Colombia. SIC emphasised that the measures should be effective and meet the standards of data security required under the Colombian Data Protection Law, and required the company to provide a certificate issued by an independent data security expert. SIC's order raise significant jurisdictional question, since the

Colombian Data Protection Law does not apply to processing that occurs outside of Colombia (and there was no allegation that any processing in violation of the Law occurred in Colombia).[172a]

Through 2020, SIC also imposed a number of fines on various companies for non-compliance with data protection rules. Some of the biggest and most notorious fines were imposed on a health company[173] and on financial institutions[174]

4. Mexico

Since the beginning of the COVID-19 pandemic, the Mexican data protection authority, the National Institute of Transparency, Access to Information and Data Protection ("**INAI**") began a series of actions to provide information to the general public on how to protect their personal data and the guidelines for data controllers on how to process personal and sensitive personal data.

Among these actions, it became imperative to announce to health-related data controllers, public and private hospitals, to comply with their legal obligations as per the Mexican data protection laws, on how to process personal data of patients diagnosed with COVID-19. This was especially the case because Mexican data protection laws consider health-related data to be sensitive and thus require stronger security measures.

One of the first actions by the Mexican data protection authority was that, on 29 March, 2020, it launched a COVID-19 microsite[175] dedicated specifically to provide useful information and guidelines to protect personal data and provide transparency during the pandemic. This microsite has been a useful tool for both data subjects and data controllers to handle personal data processed as a result of the COVID-19 pandemic.

On 2 April 2020, the INAI released a statement calling for the adoption of extreme precautions with regard to personal data of COVID-19 patients.[176] Medical personnel handling such data must use strict administrative, physical and technical safeguards to avoid any loss, destruction of improper use. The INAI also recommended that only minimum necessary personal data is collected, and only for purposes of preventing and containing the spread of the virus. This communication also speaks of the responsibility that all data processors bear when handling personal data.

As the pandemic grew, on 13 July 2020, the INAI expressed its concerns on the deficiencies of the health sector in the processing of personal data of COVID-19 patients. Francisco Javier Acuña Llamas, the then President Commissioner of INAI, noted that data bases that contain COVID-19 patients must be kept for a specific period of time and not indefinitely. He established that all data transferences of sensitive personal data should be under the specificities of the Mexican data protection laws. He also recognised that the Global Privacy Assembly, to be held in Mexico in 2021, should have at its core a discussion of the impact of the pandemic.[177]

The pandemic brought a series of events that had not been taken into consideration on a regular basis, because of the pandemic many companies allowed their employees to work from home. Because of this development, on 8 April 2020, the INAI issued recommendations for the protection of personal data in a home office environment. These guidelines highlighted the need to implement security measures that

included only using computer equipment provided by the employer, not using public connections, using only official communication sites to share information, and using passwords on all equipment used at home for work-related activities.[178]

In Mexico this brought legislative changes to the Federal Labor Law[179] that now establishes how work from home is to be regulated. These modifications to the law establish both the employers and employees' obligations when working from home. This comes to show how, due to the COVID-19 pandemic, a new normality is underway and will be here to stay.

This pandemic is far from over and it poses a challenge not only to the processing of sensitive personal data, but also to the implementation of health check points in every public space or while working from home. It has changed the way organisations protect their information from any loss or improper access putting cybersecurity at the forefront for any organisation. It has changed the way organisations interact with clients and how products or services are purchased, turning evermore to an online commerce activity. This will bring challenges not only regarding companies' operations, but also how companies collect and process a data subjects' information.

5. Uruguay

On 21 February 2020, the Council of Ministers adopted Decree No.64/020 on the Regulation of Articles 37-40 of Law No. 19.670 of 15 October 2018 and Article 12 of Law No. 18.331 of 8 November 2008.[180]

The Decree regulates new personal data protection obligations with major changes, including requiring all database owners and data controllers to report security incidents involving personal data to the Uruguayan data protection authority within a maximum of 72 hours. Reports must contain relevant information relating to the security incident, including the actual or estimated date of the breach, the nature of the personal data affected and possible impacts of the breach.

The Decree establishes the obligation to assess the impact of a breach when data processing involves specially protected data, large volumes of personal data (i.e., data of over 35,000 persons) and international data transfers to countries not offering an adequate level of protection. The Decree obliges public entities, and private entities that focus on the processing of sensitive personal data or of large volumes of data, to appoint a data protection officer.

---

[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, e.g.*, https://www.cnil.fr/en/invalidation-privacy-shield-cnil-and-its-counterparts-are-currently-analysing-its-consequences (French CNIL); https://www.aepd.es/es/derechos-y-

deberes/cumple-tus-deberes/medidas-de-cumplimiento/transferencias-internacionales/comunicado-privacy-shield (Spanish AEPD).

[3] *See* https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118.pdf.

[4] *See* https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=684836.

[5] *See* https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en.

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

[7] *See* https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries.

[8] *See* https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12740-Data-protection-standard-contractual-clauses-between-controllers-processors-located-in-the-EU-implementing-act-

[9] *See* https://edpb.europa.eu/news/news/2021/edpb-edps-adopt-joint-opinions-new-sets-sccs_en#:~:text=The%20EDPB%20and%20EDPS%20have,of%20contractual%20clauses%20(SCCs).&text=The%20Controller%2DProcessor%20SCCs%20will,between%20controllers%20and%20their%20processors.

[10] *See, e.g.*, https://www.enisa.europa.eu/news/executive-news/top-tips-for-cybersecurity-when-working-remotely. On 15 March 2020, the Director of the ENISA shared some views on teleworking conditions during COVID-19. The Director recommended that individuals work with a secure Wi-Fi connection and have up-to-date security software, regularly update their anti-virus systems and make periodic backups. Employers should also provide regular feedback to their employees on the procedures to follow in case of problems.

[11] *See* https://edpb.europa.eu/sites/edpb/files/files/news/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf.

[12] *See* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020XC0417(08)&from=FR.

[13] *See* https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf

*and*https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf.

[14] *See* https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf *and*https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statementinteroperabilitycontacttracingapps_en.pdf.

[15] *See* https://edps.europa.eu/sites/edp/files/publication/20-11-17_preliminary_opinion_european_health_data_space_en.pdf.

[16] *See* https://ico.org.uk/media/2617653/apple-google-api-opinion-final-april-2020.pdf.

[17] *See* https://ico.org.uk/media/for-organisations/documents/2617676/ico-contact-tracing-recommendations.pdf.

[18] *See* https://www.cnil.fr/fr/application-stopcovid-la-cnil-tire-les-consequences-de-ses-controles *and*https://www.cnil.fr/fr/tousanticovid-la-cnil-revient-sur-levolution-de-lapplication-stopcovid.

[19] *See* https://www.cnil.fr/sites/default/files/atoms/files/deliberation_du_24_avril_2020_portant_avis_sur_un_projet_dapplication_mobile_stopcovid.pdf.

[20] *See* https://www.datenschutzkonferenz-online.de/media/pm/20200616_pm_corona_warn_app.pdf.

[21] *See* https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/contact-tracing-protecting-customer-and-visitor-details/ *and*https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/09/data-protection-guidance-for-collecting-customer-information/.

[22] *See* https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Pruefschritte_Datenuebermittlung_in_Drittlaender_nach_Schrems_II.pdf.

[23] *See* https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/coronavirus-recovery-data-protection-advice-for-organisations/.

[24] *See* https://www.cnil.fr/fr/coronavirus-covid-19-les-rappels-de-la-cnil-sur-la-collecte-de-donnees-personnelles *and*https://www.cnil.fr/fr/les-questions-reponses-de-la-cnil-sur-le-teletravail.

[25] *See* https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9282117#1.

[26] *See* https://www.dataprotection.ie/sites/default/files/uploads/2020-07/Data%20Protection%20implications%20of%20the%20Return%20to%20Work%20Safely%20Protocol.pdf.

[27] *See* https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-onderzoekt-meten-temperatuur-werknemers-tijdens-corona.

[28] *See* https://www.cnil.fr/fr/cameras-dites-intelligentes-et-cameras-thermiques-les-points-de-vigilance-de-la-cnil-et-les-regles *and*https://www.datenschutzkonferenz-online.de/media/dskb/20200910_beschluss_waeremebildkameras.pdf.

[29] *See* https://ec.europa.eu/health/sites/health/files/vaccination/docs/2019-2022_roadmap_en.pdfhttps://ec.europa.eu/health/sites/health/files/vaccination/docs/2019-2022_roadmap_en.pdf.

[30] *See* https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

[31] *See* https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-actualiza-guia-cookies.

[32] *See* https://www.cnil.fr/fr/cookies-et-autres-traceurs-la-cnil-publie-des-lignes-directrices-modificatives-et-sa-recommandation.

[33] *See* https://data.consilium.europa.eu/doc/document/ST-5008-2021-INIT/en/pdf.

[34] *See* https://www.aepd.es/es/documento/ps-00299-2019.pdf.

[35] *See* https://www.aepd.es/es/documento/ps-00032-2020.pdf.

[36] *See* https://www.cnil.fr/fr/sanctions-2250000-euros-et-800000-euros-pour-carrefour-france-carrefour-banque.

[37] *See* https://www.cnil.fr/en/cookies-financial-penalties-60-million-euros-against-company-google-llc-and-40-million-euros-google-ireland *and*https://www.cnil.fr/en/cookies-financial-penalty-35-million-euros-imposed-company-amazon-europe-core.

[38] *See* https://www.enisa.europa.eu/news/enisa-news/securing-personal-data-a-risky-business.

[39] *See* https://www.enisa.europa.eu/publications/recommendations-for-european-standardisation-in-relation-to-csa-ii/.

[40] *See* https://www.enisa.europa.eu/news/enisa-news/security-requirements-for-operators-of-essential-services-and-digital-service-providers.

[41] *See* https://www.enisa.europa.eu/news/enisa-news/spotlight-on-incident-reporting-of-telecom-security-and-trust-services.

[42] *See* https://www.enisa.europa.eu/news/enisa-news/enisa-unveils-its-new-strategy-on-cybersecurity-for-a-trusted-and-cyber-secure-europe.

[43] *See* https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/.

[44] *See* https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data-secure/.

[45] *See* https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/11/ico-fines-ticketmaster-uk-limited-125million-for-failing-to-protect-customers-payment-details/.

[46] *See* https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_bindingdecision01_2020_en.pdf *and* https://edpb.europa.eu/sites/edpb/files/decisions/final_decision_-_in-19-1-1_9.12.2020.pdf.

[47] *See* https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/.

[48] *See* https://ec.europa.eu/info/sites/info/files/draft_eu-uk_trade_and_cooperation_agreement.pdf.

[49] *See* https://www.gov.uk/guidance/using-personal-data-in-your-business-or-other-organisation.

[50] *See* https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-now-the-transition-period-has-ended/the-gdpr/international-data-transfers/.

[51] The adequacy decisions adopted by the European Commission currently cover Andorra, Argentina, Canada (commercial organisations only), Faroe Islands, Guernsey, Isle of Man, Israel, Japan (private-sector organisations only), Jersey, New Zealand, Switzerland and Uruguay.

[52] *See*https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-now-the-transition-period-has-ended/the-gdpr/international-data-transfers/.

[53] *See* Schedule 21 of the Data Protection Act 2018, as enacted by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019.

[54] *See* https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202008_onthetargetingofsocialmediausers_en.pdf *and* https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en.

[55] *See* https://datenschutz-hamburg.de/pressemitteilungen/2020/10/2020-10-01-h-m-verfahren.

[56] *See* https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9435753 and https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9485754.

[57] *See* https://www.aepd.es/es/documento/ps-00070-2019.pdf.

[58] *See* https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-11/cp200137fr.pdf.

[59] The Statistics are (in Russian) *available at*https://rkn.gov.ru/news/rsoc/news71528.htm.

[60] Press release (in Russian) *available at*https://rkn.gov.ru/news/rsoc/news71612.htm. For more information in English *see*https://www.reuters.com/article/us-russia-protonmail-idUSKBN1ZS1K8.

[61] Press release (in Russian) *available at*https://rkn.gov.ru/news/rsoc/news72026.htm.

[62] Press release (in Russian) *available at*https://rkn.gov.ru/news/rsoc/news73050.htm. For more information (in English) *see*https://www.ft.com/content/b1e76905-29f2-4ac0-99e0-7af07cef280d. For more information *see* the 2020 Privacy and Cybersecurity International Review and Outlook.

[63] Press release (in Russian) *available at*https://rkn.gov.ru/news/rsoc/news71720.htm. More information (in English) *available at*https://www.themoscowtimes.com/2020/01/31/russia-threatens-facebook-twitter-with-100k-fines-a69126.

[64] Press release (in Russian) *available at*https://mos-gorsud.ru/rs/taganskij/news/mirovoj-sudya-rajona-taganskij-rassmotrel-dela-ob-administrativnyh-pravonarusheniyah-v-otnoshenii-tvitter-ink-i-fejsbuk-ink, and https://mos-gorsud.ru/rs/taganskij/news/mirovoj-sudya-rajona-taganskij-rassmotrel-dela-ob-administrativnyh-pravonarusheniyah-v-otnoshenii-tvitter-ink-i-fejsbuk-ink. More information (in English) *available at*https://www.themoscowtimes.com/2020/02/13/russia-fines-twitter-and-facebook-63000-each-over-data-law-a69280.

[65] *See* https://www.themoscowtimes.com/2020/11/26/facebook-pays-russia-50k-fine-for-not-localizing-user-data-a72152.

[66] The law (in Russian) *available at*http://publication.pravo.gov.ru/Document/View/0001202012300050.

[67] The law (in Russian) *available at*http://publication.pravo.gov.ru/Document/View/0001202012300002.

[68] The law (in Russian) *available at*http://publication.pravo.gov.ru/Document/View/0001202012300044.

[69] The law (in Russian) *available at*http://publication.pravo.gov.ru/Document/View/0001202012300062.

[70] The Russian laws define the notion of illegal content broadly. Inter alia, illegal content is materials containing public calls for terrorist activities or publicly justifying terrorism, other extremist materials, as well as materials promoting pornography, the cult of violence and cruelty, and materials containing obscene language.

[71] The text of the Revised FADP (in German) is *available at*https://www.parlament.ch/centers/eparl/curia/2017/20170059/Schluzssabstimmungstext%203%20NS%20D.pdf.

[72] *See* Revised FADP, Article 3.

[73] *See* Revised FADP, Article 5(a).

[74] *See* Revised FADP, Article 5(c).

[75] *See* Revised FADP, Article 5(f).

[76] *See* Revised FADP, Article 5(j) and (k).

[77] *See* Revised FADP, Article 7.

[78] *See* Revised FADP, Article 9(3).

[79] *See* Revised FADP, Article 12.

[80] *See* Revised FADP, Article 14.

[81] *See* Revised FADP, Article 19.

[82] *See* Revised FADP, Article 21.

[83] *See* Revised FADP, Article 22.

[84] *See* Revised FADP, Article 24.

[85] *See* Revised FADP, Article 28.

[86] *See* Revised FADP, Articles 60-63.

[87] Press release *available at* https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-80318.html.

[88] Judgment of the Court of 16 July 2020 in Case C-311/18 - *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, available at*http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=rst&part=1&cid=9791227.

[89] Full statement (in Turkish) *available at* https://www.kvkk.gov.tr/Icerik/6843/-ALENILESTIRME-HAKKINDA-KAMUOYU-DUYURUSU.

[90] Full statement (in Turkish) *available at* https://www.kvkk.gov.tr/Icerik/6828/YURTDISINA-VERI-AKTARIMI-KAMUOYU-DUYURUSU.

[91] Full statement (in Turkish) *available at* https://www.kvkk.gov.tr/Icerik/6728/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-BAGLAYICI-SIRKET-KURALLARI-HAKKINDA-DUYURU.

[92] Full statement (in Turkish) *available at* https://www.kvkk.gov.tr/Icerik/6777/Kisilerin-Ad-ve-Soyadi-ile-Arama-Motorlari-Uzerinden-Yapilan-Aramalarda-Cikan-Sonuclarin-Indeksten-Cikarilmasina-Yonelik-Talepler-Hakkinda-Kamuoyu-Duyurusu.

[93] Full decision (in Turkish) *available at*https://kvkk.gov.tr/Icerik/6776/2020-481.

[94] Full criteria (in Turkish *available at*https://kvkk.gov.tr/SharedFolderServer/CMSFiles/68f1fb19-5803-4ef8-8696-f938fb49a9d5.pdf.

[95] Full statement (in Turkish) *available at*https://www.kvkk.gov.tr/Icerik/6765/AYDINLATMA-YUKUMLULUGUNUN-YERINE-GETIRILMESI-HAKKINDA-KAMUOYU-DUYURUSU.

[96] Full statement (in Turkish) available at https://www.kvkk.gov.tr/Icerik/6726/COVID-19-ILE-MUCADELEDE-KONUM-VERISININ-ISLENMESI-VE-KISILERIN-HAREKETLILIKLERININ-IZLENMESI-HAKKINDA-BILINMESI-GEREKENLER-2-.

[97] Full text of the Decision (in Turkish) *available at*https://kvkk.gov.tr/Icerik/6733/2020-103.

[98] Full text of the Decision (in Turkish) *available at*https://kvkk.gov.tr/Icerik/6790/2020-559.

[99] Full text of the Decision (in Turkish) *available at*https://www.kvkk.gov.tr/Icerik/6763/2020-286.

[100] Full text of the Decision (in Turkish) *available at*https://www.kvkk.gov.tr/Icerik/6739/2020-173.

[101] English text *available at*https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-draft-personal-information-protection-law-full-translation/.

[102] *See* Article 62 of the Draft PIPL.

[103] *See* Article 42 of the Draft PIPL.

[104] *See*https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_chinas_draft_personal_information_protection_law__18_november_2020_-_english_.pdf.

[105] *See* Article 29 of the Draft PIPL.

[106] CBIRC decisions (in Chinese) *available at*http://www.cbirc.gov.cn/branch/shanghai/view/pages/common/ItemDetail.html?docId=920602&itemId=1000 and

http://www.cbirc.gov.cn/branch/shanghai/view/pages/common/ItemDetail.html?docId=920603&itemId=1000.

[107] For the daft data protection legislation presented to the Ministry of Electronics and Information Technology on 27 July 2018 by the committee of experts led by Justice Srikrishna, *see*https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.

[108] Report on Non-Personal Data Governance Framework *available at* https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf

[109] *See* "Data Empowerment and Protection Architecture: A Secure Consent-Based Data Sharing Framework to Accelerate Financial Inclusion – Draft for Discussion" (August 2020), *available at*https://niti.gov.in/sites/default/files/2020-09/DEPA-Book_0.pdf.

[110] *See* the National Health Data Management Policy, *available at*https://ndhm.gov.in/assets/uploads/NDHM%20Health%20Data%20anagement%20Policy.pdf.

[111] *See* DSCI, "Work from Home – Best Practices" (18 March 2020), *available at*https://www.dsci.in/sites/default/files/DSCI-WorkfromHomeAdvisory-1.pdf.

[112] *See* DSCI, "COVID-19: Data Privacy Outlook" (24 April 2020), *available at*https://www.dsci.in/sites/default/files/DSCI_COVID19_Data_Privacy_Outlook.pdf.

[113] *See* also DSCI, "Business Resiliency and Security During COVID-19" (24 May 2020), available at https://www.dsci.in/sites/default/files/Business-Resiliency-and-Security.pdf.

[114] *See* DSCI, "Report on Data Transfers" (8 September 2020), *available at*https://www.dsci.in/sites/default/files/documents/resource_centre/DSCI-CIPL-Accountable-Data-Transfer-Report.pdf.

[115] The Discussion Paper is *available at*https://www.tec.gov.in/pdf/Whatsnew/ARTIFICIAL%20INTELLIGENCE%20-%20INDIAN%20STACK.pdf.

[116] *See* "India bans 43 more mobile apps as it takes on China" Reuters (25 November 2020), *available at*https://uk.reuters.com/article/uk-india-china-apps/india-bans-43-more-mobile-apps-as-it-takes-on-china-idUKKBN2841QI.

[117] The press release and a list of the apps that were blocked are *available at*https://pib.gov.in/PressReleasePage.aspx?PRID=1635206#.XvoIE9L3Qpw.whatsapp.

[118] The press release and a list of the apps that were blocked are *available at*https://pib.gov.in/PressReleasePage.aspx?PRID=1650669.

[119] The press release and a list of the apps that were blocked are *available at*https://www.pib.gov.in/PressReleasePage.aspx?PRID=1675335.

[120] Case BLAPL/4592/2020 Subhranshu Rout @ Gugul v State of Odisha *available at* https://www.medianama.com/wp-content/uploads/display_pdf.pdf.

[121] Press release (in Indonesian) *available at*https://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 at*https://web.kominfo.go.id/sites/default/files/users/4752/Rancangan%20UU%20PDP%20Final%20%28Setneg%20061219%29.pdf.

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

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

[124] Press release (in Hebrew) available at https://www.gov.il/he/departments/publications/Call_for_bids/amendment_privacy_protection

[125] Press release (in Hebrew) available at https://www.tazkirim.gov.il/s/law-item/a093Y00001RdRNXQA3/%D7%AA%D7%96%D7%9B%D7%99%D7%A8-%D7%97%D7%95%D7%A7-%D7%94%D7%92%D7%A0%D7%AA-%D7%94%D7%A4%D7%A8%D7%98%D7%99%D7%95%D7%AA-%D7%AA%D7%99%D7%A7%D7%95%D7%9F-%D7%9E%D7%A1-%D7%94%D7%92%D7%93%D7%A8%D7%95%D7%AA-%D7%95%D7%A6%D7%9E%D7%A6%D7%95%D7%9D-%D7%97%D7%95%D7%91%D7%AA-%D7%94%D7%A8%D7%99%D7%A9%D7%95%D7%9D-%D7%94%D7%AA%D7%A9%D7%A3-2020?language=iw

[126] *See* "Opinion regarding cross-border transfers of personal data, from Israeli based organisations to organisations based in countries complying with the data protection legislation of the EU" (1 July 2020), *available at*https://www.gov.il/en/Departments/publications/reports/personaldata_the_european_union.

[127] *See* "Personal data of all 6.5 million Israeli voters is exposed" (10 February 2020), *available at*https://www.nytimes.com/2020/02/10/world/middleeast/israeli-voters-leak.html. Press release, "Data Breach at Shirbit" (1 December 2020), *available at*https://www.gov.il/en/departments/news/news_shirbit.

[128] English version of the of APPI *available at*https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf.

[129] Department of Personal Data Protection, "Public Consultation Paper No. 10/2020 – Review of Personal Data Protection Act 2010 (Act 709)" (14 February 2020), *available at*https://www.pdp.gov.my/jpdpv2/assets/2020/02/Public-Consultation-Paper-on-Review-of-Act-709_V4.pdf. *See also* a press release of 26 August 2020, where the Malaysian government announces the continued discussions on amending the Personal Data Protection Act 2010 (in Malay), *available at*https://www.kkmm.gov.my/awam/berita-terkini/17616-bernama-26-ogos-2020-kerajaan-masih-bincang-keperluan-pinda-akta-perlindungan-data-peribadi.

[130] Advisory guidelines (in Malay) *available at*https://www.kkmm.gov.my/images/AdHoc/200529-ADVISORY.pdf.

[131] *See* "MCI and PDPC launch online public consultation on Personal Data Protection (Amendment) Bill 2020", Press Release (14 May 2020), *available at*https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2020/5/MCI-and-PDPC-launch-online-public-consultation-on--Personal-Data%20Protection-Amendment-Bill-2020; "Public Consultation on the Draft Personal Data Protection (Amendment) Bill" (28 May 2020), *available at*https://www.mci.gov.sg/public-consultations/public-consultation-items/public-consultation-on-the-draft-personal-data-protection-amendment-bill.

[132] *See* Bill No. 37/2020 *Personal Data Protection (Amendment) Bill*, *available at*https://www.parliament.gov.sg/docs/default-source/default-document-library/personal-data-protection-(amendment)-bill-37-2020.pdf; Ministry of Communications and Information, "Amendments to the Personal Data Protection Act and Spam Control Act Passed", Press Release (2 November 2020), *available at*https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2020/11/amendments-to-the-personal-data-protection-act-and-spam-control-act-passed.

[133] *See* "Opening Speech by Mr S Iswaran, Minister for Communications and Information, at the Second Reading of the Personal Data Protection (Amendment) Bill 2020 on 2 November 2020" (2 November 2020), *available at*https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2020/11/opening-speech-by-minister-iswaran-at-the-second-reading-of-pdp-(amendment)-bill-2020.

[134] *See* "Amendments to the Personal Data Protection Act and Spam Control Act Passed", Press Release (2 November 2020), *available at*https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2020/11/amendments-to-the-personal-data-protection-act-and-spam-control-act-passed.

[135] *See* PDPC, "Draft Advisory Guidelines on Key Provisions of the Personal Data Protection (Amendment) Bill" (20 November 2020), *available at*https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Draft-AG-on-Key-Provisions/Draft-Advisory-Guidelines-on-Key-Provisions-of-the-PDP-(Amendment)-Bill-(20-Nov-2020).pdf?la=en.

[136] English version of PIPA *available at*https://elaw.klri.re.kr/kor_service/lawView.do?hseq=53044&lang=ENG.

[137] Royal Decree (in Thai) *available at*http://www.ratchakitcha.soc.go.th/DATA/PDF/2563/A/037/T_0001.PDF.

[138] MDES statement (in Thai) is *available at*https://www.mdes.go.th/news/detail/2760--´ ÕÕÕÊ--àµÃÕÕÁ¤ÅÍ ´ »ÃÐ ÒÈ ÁÒµÃ¡ ÒÃ¤ÁØ¤ÃÍ §¤ÇÒÁ»ÅÍ ´ ÀÑÂ¢éÍÁÙÅÊèÇ¹ º Ø¤¤ÅÏ .

[139] MDES notice (in Thai) *available at*http://www.ratchakitcha.soc.go.th/DATA/PDF/2563/E/164/T_0012.PDF.

[140] The AGDM is a financial free zone within the UAE.

[141] *See* "Abu Dhabi Global Market Launches Public Consultation on New Data Protection Regulatory Framework" by Natasha G. Kohne, Jenny Arlington, Sahar Abas & Mazen Baddar, GDPR, International Privacy (7 December 2020), *available at* https://www.akingump.com/en/experience/practices/cybersecurity-privacy-and-data-protection/ag-data-dive/abu-dhabi-global-market-launches-public-consultation-on-new-data-protection-regulatory-framework.html.

[142] *See* "ADGM commences Public Consultation on proposed new Data Protection Regulations" (19 November 2020), *available at*https://www.adgm.com/media/announcements/adgm-commences-public-consultation-on-proposed-new-data-protection-regulations.

[143] This explanation is taken from Data Guidance – AGDM.

[144] *See* Data Protection Regulations, *available at*https://www.difc.ae/files/9315/9358/7756/Data_Protection_Regulations_2020.pdf and Data Protection Law No. 5 of 2020, *available at*https://www.difc.ae/files/6215/9056/5113/Data_Protection_Law_DIFC_Law_No._5_of_2020.pdf.

[145] For the full list of accredited GPA members, see https://globalprivacyassembly.org/participation-in-the-assembly/list-of-accredited-members/.

[146] *See* "Africa to harmonise laws for data protection, digital economy" by Gloria Nwafor, *Guardian* (8 October 2020), https://guardian.ng/appointments/africa-to-harmonise-laws-for-data-protection-digital-economy/?_sm_au_=iVV7MH8JqKDPF0RFFcVTvKQkcK8MG.

[147] *See* "Sisi endorses law on personal data protection", *Egypt Today* (18 July 2020), *available at*https://www.egypttoday.com/Article/1/89794/Sisi-endorses-law-on-personal-data-protection.

[148] Kenya's high court ruled that the country's new digital ID scheme could continue with some conditions and stronger regulations. The court banned the collection of DNA and geolocation data, *See* "Court orders safeguards for Kenyan digital IDs, bans DNA collecting", by Humphrey Malalo, Omar Mohammed, (31 January 2020), *available at*https://www.reuters.com/article/us-kenya-rights/court-orders-safeguards-for-kenyan-digital-ids-bans-dna-collecting-idUSKBN1ZU23D

[149] *See* "ITI Comments on the U.S.-Kenya Trade Agreement Negotiation" (27 April 2020), https://www.itic.org/policy/ITIUS-KenyaFTAComments_27APR2020_FINAL.pdf and "ITI: U.S.-Kenya Trade Agreement Can Set New Global Benchmark for Digital Trade" (28 April 2020), *available at*https://www.itic.org/news-events/news-releases/iti-u-s-kenya-trade-agreement-can-set-new-global-benchmark-for-digital-trade.

[150] *See* "Joint Statement Between the United States and Kenya on the Launch of Negotiations Towards a Free Trade Agreement" (7 August 2020), *available at*https://ustr.gov/node/10204.

[151] *See* "Stakeholders' Consultation Workshop on the Data Protection Bill in Namibia" (24-26 February 2020), *available at*https://www.coe.int/en/web/cybercrime/glacyplusactivities/-/asset_publisher/ekq5KxUZwAqU/content/glacy-stakeholders-consultation-workshop-on-the-data-protection-bill-in-namibia?inheritRedirect=false&redirect=https%253A%252F%252Fwww.coe.int%252Fen%252Fweb%252Fcybercrime%252Fglacyplusactivities%253Fp_p_id%253D101_INSTANCE_ekq5KxUZwAqU%2526p_p_lifecycle%253D0%2526p_p_state%253Dnormal%2526p_p_mode%253Dview%2526p_p_col_id%253Dcolumn-4%2526p_p_col_count%253D1.

[152] *See* "Pantami Reiterates FG's Commitment to Strengthening Cybersecurity" (14 April 2020), *available at*https://www.ncc.gov.ng/media-centre/news-headlines/783-pantami-reiterates-fg-s-commitment-to-strengthening-cybersecurity.

[153] *See* https://von.gov.ng/collection-of-covid-19-data-aligns-with-ndpr-guidelines-nitda/.

[154] *See* "Annual Report for the 2019/2020 Financial Year", *available at*https://www.justice.gov.za/inforeg/docs/anr/ANR-2019-2020-InformantionRegulatorSA.pdf and "South Africa must implement privacy laws to protect citizens, says UN expert" (12 March 2020), *available at*https://mg.co.za/article/2020-03-12-south-africa-must-implement-privacy-laws-to-protect-citizens-says-un-expert/. Moreover, two significant incidents were reported: Experian South Africa announced a data incident affecting 24 million South Africans and 793,749 businesses, *see* "Experian South Africa curtails data incident" (19 August 2020), *available at*https://www.experian.co.za/content/dam/marketing/emea/soafrica/za/assets/experian-south-africa-statement-19082020.pdf. Nedbank announced a data incident concerning 1.7 million clients, *see* "Nedbank warns clients of potential impact of data incident at Computer Facilities (Pty) Ltd", https://www.nedbank.co.za/content/nedbank/desktop/gt/en/info/campaigns/nedbank-warns-clients.html.

[155] *See* "Guidance Note on the Processing of Personal Information in the Management and Containment of COVID-19 Pandemic in terms of the Protection of Personal Information Act 4 of 2013 (POPIA)," *available at*https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-PPI-Covid19-20200403.pdf and Press Release (3 April 2020), *available at*https://www.justice.gov.za/inforeg/docs/ms-20200403-GuidanceNote-PPI-Covid19.pdf.

[156] *See* "Conseil des ministres: un projet de décret sur la protection des données à caractère personnel adopté" (9 December 2020), *available at*https://presidence.gouv.tg/2020/12/09/conseil-des-ministres-un-projet-de-decret-sur-la-protection-des-donnees-a-caractere-personnel-adopte/.

[157] *See* "Statement on cabinet decisions of 27th October 2020", *available at*https://www.primature.gov.rw/index.php?id=131&tx_news_pi1%5Bnews%5D=933&tx_news_pi1%5Bcontroller%5D=News&tx_news_pi1%5Baction%5D=detail&cHash=7a012c144e6b2eb6d384a0bf1f153c26.

[158] *See* "Rwanda data protection bill approved" (29 October 2020), *available at*https://iapp.org/news/a/rwanda-data-protection-bill-approved/#:~:text=30%20and%20included%20provisions%20on,as%20transfers%2C%20sharing%20and%20retention.

[159] *See* Cybersecurity Regulation n˚ 010/r/cr-csi/rura/020 of 29/05/2020, *available at*https://rura.rw/fileadmin/Documents/ICT/Laws/Cybersecurity_Regulation_in_Rwanda.pdf.

[160] *See* "Oman: Latest developments in data protection and cybersecurity," Alice Gravenor, *PWC-Middle East* (19 November 2020), *available at*https://www.pwc.com/m1/en/media-centre/articles/oman-latest-developments-data-protection-cybersecurity.html.

[161] *See* Draft Personal Data Protection Bill (9 April 2020), *available at*https://moitt.gov.pk/SiteImage/Misc/files/Personal%20Data%20Protection%20Bill%202020%20Updated(1).pdf.

[162] *See* social media rules adopted (6 October 2020), *available at*https://moitt.gov.pk/SiteImage/Misc/files/Corrected%20Version%20of%20Rules.pdf.

[163] Law (in English) *available at*https://www.lgpdbrasil.com.br/wp-content/uploads/2019/06/LGPD-english-version.pdf.

[164] Law (in Portuguese) *available at*https://www.in.gov.br/en/web/dou/-/lei-n-14.058-de-17-de-setembro-de-2020-278155040.

[165] Bill (in Portuguese) *available at*: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=E847373CA5B3CD6F9C0FEF1AA14EED13.proposicoesWebExterno1?codteor=1931814&filename=Tramitacao-PL+4695/2020.

[166] Regulation (in Portuguese) *available at* https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO760LFI_pHFdPDvhssf6GcKAE5_GJovBZUfi7_h9SO4EFu4GZ_rtRSkPAMggKV38swnbODIuh_k2ClcCwWdtg0X.

[167] Decision (in Spanish) *available at*https://www.argentina.gob.ar/sites/default/files/rs-2020-33-apn-aaip.pdf.

[168] Law (in Spanish) *available at*http://servicios.infoleg.gob.ar/infolegInternet/anexos/230000-234999/233066/norma.htm.

[169] Decision (in Spanish) *available at*https://www.argentina.gob.ar/sites/default/files/rs-2020-25457045-apn-aaip_google.pdf.

[170] Press release (in Spanish) *available at*https://www.consejotransparencia.cl/fiscalizacion-del-cplt-descubre-vulneracion-de-la-privacidad-de-pacientes-en-compras-de-hospitales-y-servicios-de-salud/.

[171] Letter (in Spanish) *available at*https://www.consejotransparencia.cl/wp-content/uploads/2020/06/N%C2%B0000746-Patricio-Ferna%CC%81ndez-Pe%CC%81rez.-Superintendente-de-Salud.pdf.

[172] Order (in Spanish) *available at*https://www.sic.gov.co/sites/default/files/files/Normativa/Resoluciones/Res%2074519%20DE%202020%20ZOOM(1).pdf.

[172a] *See* https://www.sic.gov.co/slider/superindustria-ordena-la-plataforma-zoom-reforzar-medidas-de-seguridad-para-proteger-los-datos-personales-de-los-colombianos

[173] The imposed fine was of COP 894,365,280 (approx. €214,524), after confirming the violation of the personal data of a data subject whose data was being processed by EPS. Full Resolution *available at* https://www.sic.gov.co/sites/default/files/files/Normativa/Resoluciones/1%20Apelacio%CC%81n%2018-179365%20%20EPS%20SANITAS%20VP%20F%20(1)%20(1).pdf.

[174] For the first bank, the imposed fine was of COP 702,000,000 (approx. €171,400) for including information that was not of a financial or credit nature in the credit history of 288,753 Colombians. Full Resolution *available at*https://www.sic.gov.co/sites/default/files/files/Normativa/Resoluciones/SANCIO%CC%81N%20CIFIN.pdf; for the second bank, the imposed fine was of COP 269,046,492 (approx. €60,030) for violating a data subject's right to deletion. Full Resolution of SIC *available at*https://www.sic.gov.co/sites/default/files/files/Normativa/Resoluciones/19-141889%20VP.pdf; for the third bank, the imposed fine was of COP 356,070,000 (approx. €80,910) for violations of Law 1581 of 2012 and Decree 4886 of 2011. Full decision of SIC *available at*https://www.sic.gov.co/sites/default/files/files/Noticias/2019/RE10720-2020(1).pdf.

[175] Press release (in Spanish) *available at*https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Comunicado%20INAI-102-20.pdf.

[176] Press release (in Spanish) *available at*https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Comunicado%20INAI-106-20.pdf.

[177] Press release (in Spanish) *available at*https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Comunicado%20INAI-228-20.pdf.

[178] Press release (in Spanish) *available at*https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Comunicado%20INAI-113-20.pdf.

[179] Mexico's Official Gazzete publication of January 11, 2021 that modifies section XII Bis of the Federal Labor Law
*available at*http://dof.gob.mx/nota_detalle.php?codigo=5609683&fecha=11/01/2021.

[180] Decree (in Spanish) *available at*https://www.impo.com.uy/bases/decretos/64-2020

The following Gibson Dunn lawyers assisted in the preparation of this article: Ahmed Baladi, Alexander Southwell, Alejandro Guerrero, Vera Lukic and Clémence Pugnet.

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, PCCP 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, PCCP 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)
Howard S. Hogan – Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com)

Joshua A. Jessen – Orange County/Palo Alto (+1 949-451-4114/+1 650-849-5375, jjessen@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)
Cassandra L. Gaedt-Sheckter – Palo Alto (+1 650-849-5203, cgaedt-sheckter@gibsondunn.com)