GIBSON DUNN

January 29, 2019

INTERNATIONAL CYBERSECURITY AND DATA PRIVACY OUTLOOK AND REVIEW – 2019

To Our Clients and Friends:

As every year, in honor of Data Privacy Day—an international effort to raise awareness and promote privacy and data protection best practices—we offered Gibson Dunn's seventh annual Cybersecurity and Data Privacy Outlook and Review. In addition to that U.S.-focused report, we again this year offer this International Outlook and Review.

Like many recent years, 2018 saw significant developments in the evolution of the data protection and cybersecurity landscape in the European Union ("EU"):

- Following the adoption and application of the General Data Protection Regulation governing the collection, processing and transfer of personal data in 2016 ("GDPR"),[1] the EU's main privacy body took office, in the form of the European Data Protection Board ("EDPB"). The EDPB and its predecessor, the Article 29 Working Party Group ("WP29"), issued a number of guidance documents throughout 2018 for the interpretation and application of the GDPR.

- Furthermore, several EU Member States continued to adapt their national legal frameworks, and started to apply these laws and the GDPR, since the GDPR's date of application on 25 May 2018.

- The Council of the EU, which represents the governments and administrations of the EU Member States, pursued its internal discussions regarding the adoption of an EU regulation with respect to private life and the protection of personal data in electronic communications, intended to repeal the currently applicable legal framework ("ePrivacy Regulation").

- EU Member States continued to work on the transposition and application of the EU Directive on the security of network and information systems ("NIS Directive").

- Several objections were raised by EU institutions and before EU supervisory authorities and courts regarding different frameworks for international data transfers (e.g., the EU-U.S. Privacy Shield, the European Commission's Standard Contract Clauses).

In addition to the EU, a number of different bills were introduced and passed into law in other jurisdictions around the globe, including in other local European jurisdictions, Asia-Pacific region, Canada and Latin America.

We cover these topics and many more in this year's International Cybersecurity and Data Privacy Outlook and Review. While we do not attempt to address every development that occurred in 2018, this

Review focuses on a number of the most significant developments affecting companies as they navigate the evolving cybersecurity and privacy landscape.

Table of Contents

I. European Union

A. EU GDPR: Its Main Elements, Implementation and Application

1. GDPR

On 25 May 2018, after a two-year "grace period" the GDPR became the main legislative act for the protection of personal data and privacy in the EU. The GDPR replaces the EU Data Protection Directive [2] and constitutes a set of data protection rules that are directly applicable to the processing of personal data across EU Member States.

2. Principal Elements of the GDPR

As explained in the 2018 International Outlook and Review, the GDPR brought about a significant change in all aspects of the EU's data protection regime, revamping the substantive provisions regarding data protection law compliance and further developing and integrating the application and enforcement aspects of it. The core substantive elements of the GDPR include the following:

- **Extraterritorial Scope**: The GDPR applies not only to data controllers established in the EU, but also to organizations that either offer goods or services to individuals located in the EU or monitor their behavior, even if these organizations are not established in the EU and do not process data using servers in the EU. [3] On 23 November 2018, the EDPB published draft Guidelines on the territorial scope of the GDPR, which were subject to public consultation. [4]

- **Transparency Principle**: Under the GDPR, transparency is a general requirement applicable to three central areas: (i) the provision of information to data subjects; (ii) the way data controllers communicate with data subjects in relation to their rights under the GDPR; and (iii) how data controllers allow and facilitate the exercise of their rights by data subjects. In April 2018, the WP29 published its Guidelines on transparency, which emphasized the importance of providing data subjects with clear and full information, comprehensible to the average data subject, and made available in layers. [5]

- **Consent of the Data Subjects**: The GDPR put emphasis on the notion of consent of data subjects by providing further clarification and specification of the requirements for obtaining and demonstrating valid consent. In April 2018, the WP29 adopted Guidelines specifically dedicated to the concept of consent and focusing on the changes in this respect resulting from the GDPR. [6] In these Guidelines, the WP29 emphasized the importance of consent being obtained *freely*, and questioned the relevance of "consent" as a legal basis for data processing where consumers are, in practice, obliged to provide their personal data to, for example, engage and receive a service.

- **Right to Be Forgotten**: The GDPR further develops the "right to be forgotten" (formally known as the "right to erasure"), whereby personal data must be deleted when an individual no longer wants his or her data to be processed by a company and there are no legitimate reasons for retaining the data. [7] This right was already introduced in the EU Data Protection Directive, and was the object of the litigation before the Court of Justice of the EU ("CJEU") in *Google Spain SL and Google Inc. v. AEPD and Mario Costeja González*. [8]

  Among other points, the GDPR clarifies that this right is not absolute and will always be subject to the legitimate interests of the public, including the freedom of expression and historical and scientific research. The GDPR also obliges controllers who have received a request for erasure to inform other controllers of such request in order to achieve the erasure of any links to or copy of the personal data involved. This part of the GDPR may impose significant burdens on affected companies, as the creation of selective data destruction procedures often leads to significant costs.

- **Data Breach Notification Obligation**: The GDPR requires data controllers to provide notice of serious security breaches to the competent supervisory authorities, also known as Data Protection Authority/ies ("DPA(s)"), without undue delay and, in any event, within 72 hours after becoming aware of any such breach. The WP29 has issued Guidelines in order to explain the mandatory breach notification and communication requirements of the GDPR as well as some of the steps data controllers and data processors can take to meet these new obligations. [9]

- **Profiling Activities**: The GDPR specifically addresses the use of profiling and other automated individual decision-making. In February 2018, the WP29 issued Guidelines clarifying the provisions of the GDPR regarding profiling, in particular by defining in more detail what profiling is. [10] .

- **Data Protection Impact Assessment (**"DPIA"**)**: Where processing activities are deemed likely to result in high risk to the rights and freedoms of data subjects, the GDPR requires that data controllers carry out, prior to the contemplated processing, an assessment of the impact thereof on the protection of personal data. [11] However, the GDPR does not detail the specific criteria that needs to be taken into account to determine whether any given processing activities represent a "high risk". Instead, the GDPR only provides a non-exhaustive list of examples falling within this scope. Similarly, no process for performing DPIAs is detailed in the GDPR. Considering the need for additional information in this respect, the WP29 issued Guidelines in October 2017 intended to clarify which processing operations must be subject to DPIAs and how they should be carried out. [12]

- **Privacy-Friendly Techniques and Practices**: "Privacy by design" is the idea that a product or service should be conceived from the outset to ensure a certain level of privacy for an individual's data. "Privacy by default" is the idea that a product or service's default settings should help ensure privacy of individual's data. The GDPR establishes privacy by design and privacy by default as essential principles. Accordingly, businesses should only process personal data to the extent necessary for their intended purposes and should not store it for longer than is necessary for those purposes. These principles will require data controllers to design data protection safeguards into their products and services from the inception of the product development process.

- **Data Portability**: The GDPR establishes a right to data portability, which is intended to make it easier for individuals to transfer personal data from one service provider to another.

  According to the WP29, as a matter of good practice, companies should develop the means that will contribute to answering data portability requests, such as download tools and Application Programming Interfaces. Companies should guarantee that personal data is transmitted in a structured, commonly used and machine-readable format, and they should be encouraged to ensure the interoperability of the data format provided in the exercise of a data portability request. In April 2017, the WP29 issued Guidelines on the right to data portability providing guidance on the way to interpret and implement the right to data portability introduced by the GDPR. [13]

- **Competent Supervisory Authority**: To date, the monitoring of the application of EU data protection rules has fallen almost exclusively on the national DPAs. With the adoption of the GDPR, a complex set of rules has been established to govern the applicability of the rules to data controllers that have cross-border processing practices.

- *First*, where a case relates only to an establishment of a data controller or processor in a Member State or substantially affects residents only in a Member State, the DPA of the Member State will have jurisdiction to deal with the case. [14]

- *Second*, in other cases concerning cross-border data processing, the DPA of the main establishment of the controller or processor within the EU will have jurisdiction to act as *lead* DPA for the cross-border processing of this controller or processor. [15] Articles 61 and 62 provide for mutual assistance and joint operations mechanisms, respectively, to ensure compliance with the GDPR. Furthermore, the lead DPA will need to follow the cooperation mechanism provided in Article 60 with other DPAs "concerned". Ultimately, the EDPB (where all EU DPAs and the European Commission are represented) will have decision-making powers in case of disagreement among DPAs as to the outcome of specific investigations. [16]

- *Third*, the GDPR establishes an urgency procedure that any DPA can use to adopt time-barred measures regarding data processing in case of urgency. These measures will only be applicable in the DPA's own territory, pending a final decision by the EDPB. [17]

- In 2017, the WP29 issued Guidelines that aim to assist controllers and processors in the identification of their lead DPA. [18]

- **Governance**: Data controllers and processors may be required to designate a Data Protection Officer ("DPO") in certain circumstances. Small and medium-sized enterprises are exempted from the obligation to appoint a DPO insofar as data processing is not their core business activity. In April 2017, the WP29 issued Guidelines that clarify the conditions for the designation, position and tasks of the DPO to ensure compliance with the GDPR. [19]

These requirements will be supplemented by a much more rigid regime of fines for violations. DPAs will be able to fine companies that do not comply with EU rules up to EUR 20 million or up to 4% of their global annual turnover, whichever is higher.

3. Guidance Adopted by the Former WP29 and the Current EDPB

As indicated above, the main EU data protection body under the now repealed EU Data Protection Directive—the WP29—has been replaced by the current EDPB, which took office on 25 May 2018.

Both the WP29, until 25 May, and the EDPB, from 25 May onwards, have subjected to public consultation and adopted certain Guidelines on the interpretation and application of certain key provisions and aspects of the GDPR. These Guidelines, some of which have been discussed in sub-section I.A.2 above, include the following: [20]

- GDPR applicability: EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - version for public consultation.

- Requirements to obtain valid consent: Guidelines on consent under Regulation 2016/679, WP259 rev.01.
- Information and transparency obligations: Guidelines on transparency under Regulation 2016/679, WP260 rev.01.
- Automated decision-making and profiling: Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251 rev.01.
- Right to data portability: Guidelines on the right to data portability under Regulation 2016/679, WP242 rev.01.
- Data breach notification obligations: Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01.
- Data protection impact assessment : Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248 rev.01.
- Data Protection Officers : Guidelines on Data Protection Officers ("DPO"), WP243 rev.01.
- Derogations to maintain records of processing activities: Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR.
- Certification bodies and criteria:
    - EDPB Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679).
    - EDPB Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679 - version for public consultation.
- Transfers of personal data outside the EU:
    - EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679.
    - Working Document Setting Forth a Co-Operation Procedure for the approval of "Binding Corporate Rules" for controllers and processors under the GDPR, WP 263 rev.01.
    - Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, WP 264.
    - Recommendation on the Standard Application form for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, WP 265.

- Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, WP 256 rev.01.
- Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP 257 rev.01.
- Adequacy Referential, WP 254 rev.01.

· Identification of the lead DPA: Guidelines for identifying a controller or processor's lead supervisory authority, WP244 rev.01.

· Fines and penalties imposed by DPAs: Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, WP 253.

4. National Data Protection Initiatives Implementing and Applying the GDPR

Because the GDPR is a regulation, there is no need for EU Member States to transpose its provisions in order to render them applicable within their national legal systems. However, some Member States nonetheless have adapted their legal frameworks regarding data protection in light of the GDPR.

The GDPR contains provisions granting flexibility to the Member States to implement such adaptations. For example, Article 8 of the GDPR provides specific rules regarding the processing of personal data of children below the age of 16. Nevertheless, Member States may provide by law for a lower age provided it is not below 13 years. Article 88 of the GDPR also enables Member States to set out more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context.

Below is an overview of the national data protection reforms implemented throughout the EU during 2018:

Member State	**National Data Protection Law Adopted**
Austria	Federal Act on the Protection of Individuals with regard to the Processing of Personal Data (the "Data Protection Act" (DSG)), BGBI. I No. 165/1999), of 17 August 1999.
Belgium	– Law on the creation of the Data Protection Authority, of 3 December 2017 (the "Institutional Law"). – Law on the protection of natural persons with regard to the processing of personal data, of 30 July 2018 (the "Substantive Law").

Member State	National Data Protection Law Adopted
	– Law on economic matters which introduces collective redress action, of 30 July 2018 (the "Collective Redress Law"). – Law on the installation and use of cameras, of 21 March 2018 (the "Camera Law") [modifying the Law of 21 March 2017]. – Law on the creation of an Information Security Committee, of 5 September 2018 (the "Information Security Law").
Bulgaria	On 30 April 2018, a draft law was introduced for public consultation, amending and supplementing the Personal Data Protection Act of 4 January 2002. Public consultations ended on 30 May 2018, and the draft law submitted to the Parliament, where it is subject to further amendments.
Croatia	Act on the Implementation of the General Data Protection Regulation, of 27 April 2018.
Cyprus	Law on the Protection of Physical Persons Against the Processing of Personal Data and Free Movement of such Data, Law 125(I)/2018.
Czech Republic	Draft of the new Data Protection Act (the "DPA"), intended to adapt the current national legal framework to the GDPR. The DPA is in the legislative process, currently in the second reading in the Chamber of Deputies (lower chamber of the Czech Parliament). The DPA is expected to replace the current act on data protection.
Denmark	Danish Act on Data Protection, of 17 May 2018.
Estonia	– Personal Data Protection Act (the "PDPA"), of 12 December 2018. – Personal Data Protection Implementation Act.
Finland	Data Protection Act of Finland, which entered into force on 1 January 2018. Some minor amendments will be made to the Working Life Act (which aims to promote the protection of privacy and other rights safeguarding the privacy in working life) and a Government Proposal regarding these amendments has been given in July 2018. The amendments have not yet been passed, but the objective is that the amended act shall enter into force as soon as possible.

Member State	National Data Protection Law Adopted
France	– Ordinance No. 2018-1125, of 12 December 2018 – Law No. 2018-493 on the protection of personal data, of 20 June 2018. – Decree No. 2018-687, of 1 August 2018.
Germany	German Federal Data Protection Act, of 5 July 2017.
Greece	Greece has not yet issued a national law implementing the GDPR. On 5 March 2018, a public consultation on the new law was completed; however, the draft has not yet been submitted to the Greek Parliament.
Hungary	Amendment to the Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information.
Ireland	Data Protection Act 2018, of 24 May 2018.
Italy	– Law No. 163, of 6 November 2017, adopting specific provisions with respect to the GDPR. – Legislative Decree 101/2018, of 10 August 2018.
Latvia	Personal Data Processing Law, of 21 June 2018.
Lithuania	Law on Legal Protection of Personal Data, of 16 July 2018.
Luxembourg	Law on the organization of the National Data Protection Commission ("CNPD"), of 1 August 2018.
Malta	Data Protection Act 2018 (Chapter 586 of the Laws of Malta), of 28 May 2018, and the Regulations issued under it.
Netherlands	Dutch GDPR Implementation Act, of 16 May 2018.
Poland	Personal Data Protection Act, of 24 May 2018.

Member State	National Data Protection Law Adopted
Portugal	On 26 March 2018, the Portuguese government published a Draft Law (the "Draft") for the implementation of the GDPR and associated national derogations. On 3 May 2018, the Draft was submitted to the Portuguese Parliament for discussion and is currently being studied by a special group of the Portuguese Parliament. The applicable law is still Law no. 67/98, of 26 October (as amended by Law 103/2015, of 24 August) on personal data protection.
Romania	Law no. 190/2018 on the measures for the application of the GDPR.
Slovakia	– Act No. 18/2018 Coll. on the Protection of Personal Data which implements the GDPR was adopted by the Slovak Parliament on 29 November 2017. It was published in the Collection of Laws on 30 January 2018, and entered into force on 25 May 2018. – The Decree of the Office for Personal Data Protection no. 158/2018 Coll. on Data Protection Impact Assessment Procedure.
Slovenia	The new Slovenian Data Protection Act (the "ZVOP-2") is currently in the legislative pipeline, and it will repeal the current Data Protection Act (the "ZVOP-1").
Spain	Organic Law 3/2018 on the protection of personal data and guarantee of digital rights, of 5 December 2018.
Sweden	Data Protection Act (2018:218) with its complementary provisions (2018:19), of 19 April 2018.
United Kingdom	Data Protection Act 2018, of 23 May 2018.

5. GDPR cases, investigations and enforcement

In the course of 2018, EU data protection authorities continued their enforcement action against companies and organizations for violations of their pre-GDPR legal regimes (i.e., under the EU Data Protection Directive). Furthermore, soon after the GDPR became applicable and Member States adapted their legal frameworks regarding data protection in light of the GDPR, investigations regarding data breaches and potential infringements of the GDPR rules started to be conducted. The most significant cases are set out below.

a) Data breaches and investigations

In the **UK**, the Information Commissioner's Office ("ICO") has been particularly active in the investigation of unauthorized or illegal accesses or loss of personal data.

In early 2017, a number of media reports in *The Observer* newspaper claimed that a data analytics service had worked for the Leave.EU campaign during the EU referendum, providing data services that supported micro-targeting of voters. In March 2017, the ICO announced that it would begin a review of evidence as to the potential risks arising from the use of data analytics in the political process. Following that review of the available evidence, the ICO announced in May 2017 that a broader formal investigation into the use of data analytics in political campaigns would be launched, in order to ascertain if there had been any misuse of personal data and breaches of data protection law by the campaigns, on both sides, during the referendum. In addition to the potential links between this data analytics organization and Leave.EU, which gave rise to the investigation, the ICO later found further lines of enquiry covering 30 organizations.

According to an official investigation update, the investigation is considering both regulatory and criminal issues, namely failure to properly comply with the Data Protection Principles, failure to properly comply with the Privacy and Electronic Communications Regulations and potential offences under the Data Protection Act 1998. [21]

So far, although the investigation is still ongoing, the ICO has issued one of the organizations involved with a monetary penalty in the sum GBP 500,000 for lack of transparency and security issues relating to the collection, processing and storage of data, constituting breaches of the first and seventh data protection principles under the Data Protection Act 1998. [22]

In November 2018, the ICO also announced it was investigating an international hotel management company after a data breach had been brought to its attention. According to public sources, personal data including credit card details, passport numbers and the dates of birth of up to 300 million people had been stolen in a cyber-attack to the parent company of the international hotel management company. [25]

In **France**, the company "Optical center" was fined EUR 250,000 by the French National Data Protection Commission ("CNIL") for failing to secure its website. Through its website it was possible to access hundreds of customer invoices, containing health data and, in some cases, the social security number of the data subjects concerned. This case is one of the highest sanctions ever pronounced by the CNIL before the GDPR came into force and illustrates the seriousness with which the CNIL is approaching data protection and data breach violations.

In another matter from before the application of the GDPR, in **Hungary**, the Hungarian regulator imposed a fine of up to HUF 20 million (approx. EUR 62,000, being the maximum fine under the Hungarian Act implementing the EU Data Protection Directive) on the Hungarian Church of Scientology for serious breaches of the local Data Protection Act.

b) GDPR investigations

In addition to the cases mentioned above, GDPR investigations have also proliferated in most of the Member States based on facts occurring and being brought to the attention of supervisory authorities after 25 May 2018.

On 25 and 28 May 2018, in **France** the CNIL received group complaints from the associations None Of Your Business and La Quadrature du Net. In these complaints, the associations complained against Google LLC for not having a valid legal basis to process the personal data of the users of its services, particularly for the purposes of customizing and delivering targeted ads. After an investigation period and on the basis of online inspections conducted, CNIL stated that in this context two types of GDPR breaches had occurred, namely a breach of transparency and information obligations; and a violation of the obligation to have a legal basis for customizing and delivering targeted ads. On these grounds, the CNIL imposed a financial penalty of EUR 50 million to Google LLC on 21 January 2019. [26]

In particular, the CNIL considered that Google users were not able to fully understand the scope of the processing operations carried out by Google LLC and that the purposes of these processing operations were described in a too generic and vague manner. Similarly, the information communicated was considered to be not clear enough so that the user can understand that the legal basis of processing operations for the ad targeting is consent, and not the legitimate interest of the company. Finally, the CNIL noticed that information on data retention periods was not provided for some categories of data. [27]

In **Ireland**, an online news and social networking service is currently being investigated by Irish privacy authorities over its refusal to give a user information about how it tracks users when they click on links posted on the service. The company refused to disclose the data it recorded when a user clicked on links in other people's links, claiming that providing this information would take a disproportionate effort. In December 2018, the Irish Data Protection Commission opened a statutory inquiry into the company's compliance with the relevant provisions of the GDPR following receipt of a number of breach notifications from the company since the introduction of the GDPR. [28]

B. International Transfers: Adequacy Declarations and Challenges

1. Adequacy Declarations

Both under the former EU Data Protection Directive and the current GDPR, transfers of personal data outside of the EU are generally prohibited unless, *inter alia*, the European Commission formally concludes that the legislation of the country of destination of the data protects it adequately. Thus far, the European Commission has only recognized the following countries to provide adequate protection to personal data: Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the U.S. (limited to the EU-U.S. Privacy Shield framework). [29]

In the course of 2018, adequacy talks have proceeded with regard to two major Asian economies: Japan and South Korea.

a) Japan

With regard to Japan, negotiations with the EU on the finding of reciprocal adequacy took place in the course of the last years, and ended on 17 July 2018. Upon the conclusion of these negotiations, the EU and Japan both agreed to recognize each other's regimes for the protection of personal data as being adequate, thereby enabling safe transfers of personal data between the EU and Japan. This arrangement is meant to complement the EU-Japan Economic Partnership Agreement, [30] enabling European and Japanese companies to benefit from free data flows, as well as from privileged access to approximately 650 million European and Japanese consumers.

On 5 September 2018, the European Commission formally launched the procedure for the finding of adequacy of the data protection regime in Japan. [31] In issuing its draft adequacy decision to cover transfers of personal data to Japan, the European Commission highlighted the following commitments that Japan made to improve the protection of EU personal data:

- Japan committed to adopt a set of rules, providing individuals in the EU whose personal data are transferred to Japan with additional safeguards that will bridge several differences between the data protection systems of both jurisdictions. These additional safeguards will strengthen, for example, the protection of sensitive data, the conditions under which EU data can be further transferred from Japan to another third country, and the exercise of individual rights to access and rectification. These rules will be binding on Japanese companies importing data from the EU, and they will be enforceable by the Japanese independent data protection authority and by Japanese courts.

- The Japanese government also gave assurances to the EU regarding safeguards concerning the access of Japanese public authorities for criminal law enforcement and national security purposes, ensuring that any use of personal data would be limited to what is necessary and proportionate, and subject to independent oversight and effective redress mechanisms.

- Japan committed to implement a complaint-handling mechanism to investigate and resolve complaints from Europeans regarding access to their data by Japanese public authorities. This new mechanism will be administered and supervised by the Japanese independent data protection authority.

On 5 December 2018, the EDPB issued its opinion on the draft adequacy decision prepared by the European Commission with regard to Japan. [32] Although the EDPB praised the efforts of the European Commission to reach an understanding with the Japanese government, a number of outstanding points were identified as being crucial for the finding of adequacy of the Japanese data protection regime. In particular:

- The EDPB remarked that the system for the monitoring of the new architecture of adequacy, which combines the existing Japanese legal framework with specific Supplementary Rules applicable to EU personal data, will pose certain challenges to ensure compliance by Japanese entities and enforcement by the Personal Information Protection Commission ("PPC").

- The EDPB raised some concerns regarding the possibility of onward transfers of EU data from Japan to third countries that are only subject to a Japanese adequacy decision, but not to an adequacy decision from the European Commission.

- The EDPB also expressed some concerns in relation to the consent and transparency obligations of data controllers. As opposed to EU data protection law, the use of consent as a basis for the processing and transfer of personal data has a central role in the Japanese legal system. Some inconsistencies in the definition of consent under EU and Japanese law, such as the existence of "free" consent or the introduction of the right to withdraw consent, could be interpreted to cast doubt on data subjects' ability to genuine control over their personal data.

- The EDPB raised some questions regarding the availability and accessibility of the "helpline" of the Japanese data protection authority for EU data subjects. Certain important documentation is only available in the Japanese-language version of official websites, if at all, which will raise challenges in the reliance of EU data subjects on Japanese data protection regulations.

In addition to the opinion issued by the EDPB, the draft adequacy decision will be subject to the following procedure:

- Consultation of a committee composed of representatives of the Member States (comitology procedure);

- Update of the European Parliament Committee on Civil Liberties, Justice and Home Affairs;

- Adoption of the adequacy decision by the College of Commissioners.

b) South Korea

Negotiations between the EU and South Korea authorities occurred in the course of 2018 with a view to adopting an adequacy decision. Although the negotiations remained confidential so far, it has been reported that the main concerns of the EU authorities are relating to the independence and powers of the South Korean data protection authority. [33] While the Personal Information Protection Act of 2011 created a Personal Information Protection Commission, the independence of this body, which lacks enforcement powers, has been questioned. The South Korean Homeland and Security Ministry is tasked with the enforcement of the Personal Information Protection Act.

On 15 November 2018, some amendments to the Personal Information Protection Act were submitted to the South Korean National Assembly, in order to grant enforcement power and functions to the Personal Information Protection Commission.

2. Challenges to Data Transfer Systems

a) Challenges to Standard Contract Clauses

As noted in the 2018 International Outlook and Review, on 3 October 2017, the Irish High Court referred the issue of the validity of the standard contractual clauses decisions to the CJEU for a preliminary ruling. [34] The proceedings before the EU are still ongoing, and a ruling is expected in 2019 or 2020.

If the CJEU decides to invalidate the standard contractual clauses, this ruling would, in all likelihood, have a tremendous impact on businesses around the world, many of which relying on these legal guarantees to ensure an adequate level of data protection to data transfers outside the EU.

b) Challenges to the EU-U.S. Privacy Shield

On 12 July 2016, the European Commission formally approved the EU-U.S. Privacy Shield, a framework for navigating the transatlantic transfer of data from the EU to the United States. The Privacy Shield replaced the EU-U.S. Safe Harbor framework, which was invalidated by the CJEU on 6 October 2015 in the case *Maximilian Schrems v. Data Protection Commissioner*. [35] We provided an in-depth explanation of the Privacy Shield and a discussion of the Schrems decision in the 2018 International Outlook and Review.

Since the adoption of the Privacy Shield program in 2016, approximately 4,000 companies have adhered to the Privacy Shield framework, making legally enforceable commitments to comply with the Privacy Shield rules and principles. However, the success of the Privacy Shield has not sheltered it from certain challenges that have been directed from politicians, DPAs and individuals across Europe.

On 16 September 2016, Digital Rights Ireland Ltd., an organization that had been successful in obtaining the repeal of other EU legislation concerning personal data, [36] brought an action against the European Commission decision approving the EU-U.S. Privacy Shield. On 22 November 2017, the CJEU declared the action inadmissible, thereby giving some relief to the companies relying on this framework to transfer personal data to the U.S.

Notwithstanding this, on 5 July 2018 the European Parliament voted a non-binding resolution recommending the suspension of the EU-U.S. Privacy Shield unless certain corrective actions were adopted by the U.S. administration, including: aligning fully the Privacy Shield to the GDPR, and making the Privacy Shield fully compliant with the recommendations issued by the WP29 on 28 November 2017. [37]

In October 2018, EU Commissioner Věra Jourová, Secretary of Commerce Wilbur Ross, and members of the respective EU and U.S. administrations and authorities met with the occasion of the second annual review of the Privacy Shield. [38] During these meetings, the governments of both jurisdictions discussed the nomination and functioning of the Privacy and Civil Liberties Oversight Board and of the Privacy Shield Ombudsman Mechanism, which are important elements to guarantee the application and enforcement of the Privacy Shield.

Finally, it is notable that although the case before the CJEU from the referral from the Irish High Court concerns primarily standard contract clauses, a number of the questions posed by the Court refer to the adoption of the Privacy Shield and its influence in the overall assessment of standard contract clauses.

C. EU Cybersecurity Directive

1. Adoption and Implementation of the EU CybersSecurity Directive

In the EU, cybersecurity legislation addressing incidents affecting essential service and digital service providers is primarily covered by the NIS Directive [39], adopted on 6 July 2016.

As it was explained in the 2018 International Outlook and Review, the NIS Directive is the first set of cybersecurity rules to be adopted at the EU level, adding to an already complex array of laws with which companies must comply when implementing security and breach response processes. It aims to set a minimum level of cybersecurity standards and to streamline cooperation between EU Member States at a time of growing cybersecurity breaches.

The NIS Directive is not directly applicable by authorities and courts, and contained a deadline for Member States to transpose it into national law by May 2018. Thus, in the course of the last year, Member States have endeavored to adopt the necessary regulations and empower the appropriate authorities to transpose, apply and enforce the NIS Directive.

The final text of the NIS Directive sets out separate cybersecurity obligations for (i) *essential service* and (ii) *digital service providers*:

- Essential service providers include actors in the energy, transport, banking and financial markets, as well as health, water and digital infrastructure [40] sectors.

- Digital service providers will include online marketplaces, search engines and cloud services (with an exemption for companies with less than 50 employees) but *not* social networks, app stores or payment service providers.

The clear aim of the NIS Directive is to harmonize the EU Member State rules applicable to the security levels of network and information systems across the EU. However, given the strategic character of certain services covered by the NIS Directive, it confers some powers and margin of discretion to Member States. For example, the NIS Directive mandates each EU Member State to adopt a national strategy on the security of network and information systems, defining objectives, policies and measures envisaged with a view to achieve the aims of the NIS Directive. [41] Thus, despite the ability of Member States to seek the assistance of the European Union Agency for Network and Information Security ("ENISA"), the development of a strategy will remain a national competence. Furthermore, as far as *operators of essential services* are concerned, EU Member States will identify the relevant operators subject to the NIS Directive and may impose stricter requirements than those laid down in the NIS Directive (in particular with regard to matters affecting national security). [42]

In contrast, Member States should *not* identify *digital service providers* (as the NIS Directive applies to all digital service providers within its scope) and, in principle, may not impose any further obligations to such entities. [43] The European Commission retains powers to adopt implementing rules regarding the application of the security and notification requirements rules applicable to digital service providers. [44] It is expected that these rules will be developed in cooperation with the ENISA and stakeholders, and will enable an uniform treatment of digital service providers across the EU. In addition, the competent authorities will only be able to carry out supervisory activities when there is evidence that a digital service provider is not complying with its obligations under the NIS Directive.

Another tool for coordination among authorities will be the envisaged "**Cooperation Group**", similar to the WP29 operating currently under the 1995 Data Privacy Directive. The Cooperation Group will bring together the regulators of all EU Member States, who have different legal cultures and hold different approaches to IT and security matters (e.g., affecting national security). It is therefore expected that the European Commission will play an active role in building trust and consensus among the Cooperation Group's members with a view of providing meaningful and clear guidance to businesses.

2. Documents and Guidance Issued by ENISA

In the course of 2018, ENISA has been particularly active in issuing guidance and evaluating the responsiveness of the EU authorities, stakeholders and systems in responding to cyberattacks. In particular:

- ENISA has published a number of guidance documents aimed to assist private parties in their evaluation of security measures adopted in application of EU instruments, such as the NIS Directive [45] and the Open Internet Regulation. [46]

- Following the trends for increased use of consumer products and services relying on cloud services and Internet of Things, ENISA has issued a number of guidance documents providing companies with an overview of the potential risks and redress measures in this context. This includes the "Good practices for Security of Internet of Things in the context of Smart Manufacturing", of November 2018, [47] or the working document "Towards secure convergence of Cloud and IoT", of September 2018. [48]

- On 6-7 June 2018 ENISA held Cyber Europe 2018, a yearly exercise that simulates an intense realistic crisis caused by a large number of cybersecurity incidents. During the exercise, the EU Member States' cooperation was found to have improved at technical level and be efficient. However, ENISA also noted that the private sector had to prioritize investing on IT security, particularly in regards to essential service operators. [49]

D. Other EU Developments

1. Reform of the ePrivacy Directive – the Draft EU ePrivacy Regulation

As it was explained in the 2018 International Outlook and Review, 2016 saw the initiation of the procedures for the reform of the EU's main set of rules on ePrivacy, the ePrivacy Directive. In this

context, further to a public consultation held by the European Commission, the first proposal of the future EU ePrivacy Regulation (the "draft ePrivacy Regulation") was released on 10 January 2017. [50] In 2017, the draft ePrivacy Regulation was subject to an opinion of the WP29 (4 April 2017) [51] and an amended version issued by the European Parliament (20 October 2017). [52]

Since then, in the course of 2018, internal discussions have been ongoing at the level of the Council of the EU, which have concluded in the issuance of two final versions of the draft ePrivacy Regulation, dated 10 July and 19 October 2018. Due to the progress made, the ePrivacy Regulation is expected to be adopted in 2019.

a) The European Commission's ePrivacy Regulation Proposal

The Commission's ePrivacy Regulation proposal released in January 2017 sought to accommodate the reform of the ePrivacy regime to the feedback received from stakeholders and the WP29. In summary, the draft ePrivacy Regulation prepared by the European Commission constituted a more comprehensive piece of legislation that aims to fix and close certain open issues identified in the application of the ePrivacy Directive:

- **Regulation *versus* Directive**: The European Commission's proposal to replace the ePrivacy Directive with a Regulation means that its terms will in principle apply directly across all EU Member States, and will not require transposition at national level (e.g., via the adoption of laws by the parliaments of the different Member States). This decision is consistent with the approach adopted with regard to the GDPR. Although Member States will still be given some freedom to deviate from the ePrivacy Regulation (particularly in the area of national security), the choice to adopt a Regulation will increase the homogeneous application of the ePrivacy Regulation across all EU Member States.

- **Alignment with the GDPR**: A number of provisions in the draft ePrivacy Regulation of the European Commission demonstrated alignment with the GDPR. For example, as the GDPR, the draft ePrivacy Regulation had a broad territorial scope and applied to the provision of electronic communication services (e.g., voice telephony, SMS services) from outside the EU to residents in the EU.

  As indicated below, the draft ePrivacy Regulation also aimed to close the gap with the GDPR from an enforcement perspective, by empowering DPAs to monitor the application of the privacy-related provisions of the draft ePrivacy Regulation under the conditions established in the GDPR.

  From a substantive perspective, the definition of a number of legal concepts used in both the GDPR and the draft ePrivacy Regulation were also aligned (e.g., the conditions for "consent", the "appropriate technical and organization measures to ensure a level of security appropriate to the risks").

- **Inclusion of OTT Service Providers**: In response to the feedback of stakeholders, the draft ePrivacy Regulation indicates that the new Regulation will apply to providers of services that run

over the Internet (referred to as "over-the-top" or "OTT" service providers), such as instant messaging services, video call service providers and other interpersonal communications services. [53]

- **Cookies and Other Connection Data**: Like the ePrivacy Directive, the draft ePrivacy Regulation contained a provision that addressed the circumstances under which the storage and collection of data on users' devices is lawful. These practices may still be based on the prior consent obtained from users. In the absence of users' consent, according to the draft ePrivacy Regulation, it would still be possible to carry out these practices provided that: [54]
    - they serve the purpose of carrying out (not facilitating) the transmission of a communication over an electronic communications network; or
    - they are necessary (albeit not *strictly* necessary) for providing: (i) a service requested by the end user; or (ii) first-party web audience measuring.

The recitals of the draft ePrivacy Regulation suggested that the circumstances under which consent would not be required could be interpreted more broadly than under the current ePrivacy Directive. [55]

By contrast, the ePrivacy Regulation contains a new set of seemingly more stringent rules applicable to the "collection of information emitted by terminal equipment to enable it to connect to another device and/or to network equipment".

- **Supervisory Authorities and EDPB**: One of the novelties introduced by the draft ePrivacy Regulation was a section devoted to the appointment and powers of national supervisory authorities. [56] The relevant provisions clarify that the DPAs responsible for monitoring the application of the GDPR shall also be responsible for monitoring the application of the provisions of the draft ePrivacy Regulation related to privacy in electronic communications, and that the rules on competence, cooperation and powers of action of DPAs foreseen in the GDPR also apply to the draft ePrivacy Regulation.

b) The WP29 Opinion on the European Commission Proposal

Following the release of the European Commission's proposal, the WP29 issued its opinion on the proposed draft ePrivacy Regulation in April 2017. [57] While the WP29 welcomed the proposal and the choice for a regulation as the regulatory instrument, it highlighted four points of "grave concern" that would "lower the level of protection enjoyed under the GDPR" if adopted, and made recommendations in this respect concerning:

- The rules concerning the tracking of the location of terminal equipment, for instance WiFi tracking, which are inconsistent with the rules of the GDPR. The WP29 advised the European Commission to "promote a technical standard for mobile devices to automatically signal an objection against such tracking".

- The conditions under which the content and metadata can be analyzed should be limited: consent of all end-users (senders and recipients) should be the principle with limited exceptions for "purely personal purposes".

- Barriers used by some websites to completely block access to the service unless visitors agree to third-party tracking, known as "tracking walls," should be explicitly prohibited to give individuals the choice to refuse such tracking while still being able to access the website.

- Terminal equipment and software should offer "privacy protective settings" by default, in addition to allowing the user to adjust these settings.

The WP29 indicated that it expected its concerns to be addressed during the ongoing legislative process.

c) The European Parliament's Amended Proposal

In October 2017, the European Parliament proposed an amended version of the European Commission's proposed draft ePrivacy Regulation, [58] which introduced more stringent rules on the use of personal data and on the respect of users' privacy. Some of the notable changes include:

- The prohibition to block access to a service solely because the user has refused the processing of personal data which is not necessary for the functioning of the service.

- The requirement for providers of electronic communications services to ensure the confidentiality of the data, for instance with end-to-end encryption and the prohibition of backdoors.

- The requirement for browsers to block third-party cookies by default until the user has adjusted his/her cookie settings.

- The prohibition of "cookie walls" and cookie banners that prevent the use of the service unless users agree to all cookies.

d) The Proposal of the Council of the EU

In addition to the Parliament's version of the draft ePrivacy Regulation, the Council of the EU has also published a number of working proposals and amendments. The two latest documents related to the draft ePrivacy Regulation were published on 10 July and 19 October 2018, and they introduced some important changes to the proposals of the European Commission and of the European Parliament.

On 10 July 2018, the EU Council published some revisions to the draft ePrivacy Regulation, which focused primarily on the following key points: [59]

- The draft introduced the possibility for "*further compatible processing of electronic communications metadata*". This amendment suggests the broadening of the scope of permissible processing for research purposes, which would enable private parties to pursue

research and innovation. The Council of the EU also called for the draft ePrivacy Regulation to be "more future-proof", providing flexibility to enable developments in a rapidly changing digital environment.

- Other amendments made by the EU Council sought to clarify the lawfulness of processing operations carried out in the course of operators' daily business. For example, new language introduced in Article 6(2)(b) clarified that the processing of metadata for the purposes of calculating and billing interconnection payments is permitted.

- The EU Council also sought to clarify the rules applicable to the storage and processing of data on end-users' equipment. Pursuant to the Council's revisions, the responsibility for obtaining consent for the storage of a cookie or similar identifier lies on the entity that collects information from end-users' terminal equipment, such as an information society service provider or an ad network provider. However, these entities may request another party to obtain consent on their behalf. The Council's amendments also clarify that the end-user's consent to storage of a cookie or similar identifier may also entail consent for the subsequent readings of the cookie in the context of a revisit to the same website domain initially visited by the end-user.

- The EU Council suggests the deletion of the entire Article 10 of the draft ePrivacy Regulation, and the respective recitals, which obliged software providers to inform the end user whenever privacy settings are updated.

On 19 October 2018, the EU Council issued a new revised version of the draft ePrivacy Regulation, which included further edits and amendments in addition to those published in July. [60]

One of the most significant changes introduced to the draft ePrivacy Regulation is the recognition of the ability of information society services to use tracking technologies on the computers of individuals, without consent, for websites that partly or wholly finance themselves through advertisement, provided information obligations have been complied with and that the user "*has accepted this use*" of the data (as opposed to requiring full-blown consent).

The EU Council also included to the draft ePrivacy Regulation a new Article 6(1)(c), which allows the processing of electronic communications data when necessary to ensure the security and protection of terminal equipment. This and other similar changes introduced by the Council aim at achieving certain coherence between these provisions and the security obligations to which information society services are subject, enabling the latter to use security tools that need the processing of data contained in the terminal equipment without obtaining prior consent.

2. CJEU Case Law

2017 has also witnessed important cases before the CJEU on the application of the EU Data Protection Directive, the GDPR and the ePrivacy Directive.

a) The Determination of the Applicable Law and the Relevant Data Controller in the Context of Social Networks

On 5 June 2018, the CJEU delivered a ruling in *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH* which clarified the definition of data controller and the determination of the applicability of national data protection legislation and the powers of DPAs in cases concerning controllers established in multiple Member States. [61]

First, the CJEU indicated that administrators of webpages hosted by third parties (e.g., fan pages hosted by social networks) that knowingly make use of the services (e.g., audience statistics), may be considered to be (co)controllers of the data processed in the context of visitors' traffic to the webpage. In doing so, the CJEU recognized the joint responsibility of the operator of the third-party website (e.g., the social network) and the administrator of the webpage (e.g., a fan page) in relation to the processing of the personal data of visitors to that page, which is deemed to contribute to ensuring more complete protection of the rights of persons visiting a fan page.

Second, the CJEU found that, while an establishment of a controller focused on the sale of advertising space and other marketing activities may be subject to the laws and the powers of the DPA of the Member State where it is established, such laws and powers may not extend to an establishment of the same controller located in another Member State.

The judgment in *Wirtschaftsakademie* was followed by an Opinion of the EU's Advocate General Michal Bobek in *Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW e.V.*, which also addressed the question of determining who is the data controller in the context of the use of tools to collect and transmit cookie data (e.g., social plug-ins). The Advocate General found that an entity or organization which has embedded a third-party plug-in in its website, which causes the collection and transmission of the user's personal data, must be considered as a controller, even if it is unable to influence the data processing operation resulting from the functioning of the plug-in. However, the Advocate General observed that a controller's joint responsibility should be limited to those operations for which it effectively co- determines the means and purposes of the processing of the personal data.

The Advocate General proceeded to note that, where the processing of cookie data resulting from the use of plug-ins is based on the legitimate interests of controllers or third parties, legitimate interests of both the website operator and the plug-in provider should be taken into account as joint controllers, and an assessment should be made balancing those interests with the rights of the data subjects. Finally, the Advocate General concluded that the consent of the data subject has to be given to a website operator which has embedded the content of a third party, and that the EU Data Protection Directive must be interpreted as meaning that the obligation to inform also applies to that website operator, and both must be given before the data are collected and transferred. However, he noted that the extent of those obligations shall correspond with that operator's joint responsibility for the collection and transmission of the personal data.

b) Claims Assignment

As indicated in the 2018 International Outlook and Review, Mr. Schrems started legal proceedings against Facebook Ireland Limited before a court in Austria, which raised the question of whether jurisdiction was established in the domicile of a consumer claimant who was assigned claims by other consumers, thus opening up the possibility of collecting consumer claims from around the world.

On 14 November 2017, Advocate General Bobek delivered his opinion on the *Maximilian Schrems v. Facebook Ireland Limited* case pending in the CJEU. [62] Advocate General Bobek held that a consumer cannot invoke, at the same time as his own claims, claims on the same subject assigned by other consumers domiciled in other places in the same Member State, in other Member States, or in non-Member States.

On 25 January 2018, the CJEU concurred with the Advocate General's opinion, finding that a consumer cannot assert, in the courts of the place where he is domiciled, not only his own claims, but also claims assigned by other consumers domiciled in the same Member State, in other Member States or in non-Member State countries.

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

The increasing impact of digital services in Europe, as well as the overhaul brought about by the GDPR in the EU, have led certain jurisdictions in the vicinity of the EU to improve their data protection regulations.

A. Russia

Local data privacy laws have been heavily enforced, reflecting the activity of the Russian Data Protection Authority in monitoring and enforcing data protection compliance.

As of 1 July 2017, the administrative sanctions in Russia for certain privacy violations have been significantly increased. For example, data processing operations in excess of the consent provided by a data subject may result in a fine of RUR 75,000 (approx. USD 1,200; approx. EUR 1,000). Criminal prosecution and prison sanctions are also possible for certain types of privacy violations. Another type of enforcement action under Russian law is blockage of the online resources. Thus, if processing of personal data on the website or in the app violates data protection laws, access to such website/app may be restricted for Russian users upon the respective court decision. The most well-known and widely debated blockage related to LinkedIn, which has been blocked since 2016 and remains unavailable for Russian users. This is not the only example – some other websites, with smaller user bases, have been blocked in recent years.

The Russian Data Protection Authority has been targeting large digital multinationals in the last few years. For example, in 2017, Telegram was fined RUR 800,000 (approx. USD 14,000; approx. EUR 10,500) by Russian courts for failing to provide the Russian Federal Security Service with the decoding keys for access to personal data, as obliged by the Russian Data Protection Act. In doing so, the Russian courts disregarded Telegram's arguments based on its lack of control over the encoding and decoding

processes of its instant messaging service. On 22 October 2018, Russian courts rejected Telegram's appeal against the fine.

The Telegram case shows that, if the relevant technology used by a service provider (as long as the services relate to communications in the Internet) does not allow state authorities to access unencrypted information, this may be deemed a breach of Russian data protection and cybersecurity laws.

B. Switzerland

To prepare for the entry into force of the GDPR, the Swiss government has issued a draft of a new Data Protection Act (the "Draft FDPA") [63] that aims to:

– Modernize Swiss data protection law and to a certain extent, align it to the requirements of the GDPR; and,

– Maintain its adequacy status granted by the European Commission, to ensure the free flow of personal data between the EU and Switzerland.

The Draft FDPA was published by the Swiss Federal Council on 15 September 2017. The Draft FDPA, which will replace the Federal Act on Data Protection of 19 June 1992 (the "FADP"), has the following characteristics:

- The concept of "sensitive" or "special categories" of personal data under the Draft FDPA covers a wide range of categories of data, including personal data in the "intimate sphere" (e.g., fears, dreams, therapies), biometric data which clearly identifies an individual (e.g., pictures), data on administrative or criminal proceedings and sanctions, and data on social security measures. [64]

- The Draft FDPA contains a list of basic principles for the processing of personal data which are broadly equivalent to those contained in the GDPR. [65] By contrast, as opposed to the GDPR, the processing of personal data will not require any legal basis under the Draft FDPA (such as consent), unless such processing leads to an unlawful violation of privacy (i.e., the processing of personal data does not comply with the basic data processing principles).

- Similarly to the GDPR, under the Draft FDPA data subjects have the right to request access, rectification or erasure of their personal data and not to be subject to automated decision-making. [66] However, in contrast to the GDPR, the Draft FDPA does not provide for a right to data portability.

- The Draft FDPA contains a duty for companies to carry out a DPIA in specific situations, which closely mimic the scenarios envisaged by the GDPR. [67] The Draft FDPA also contains an obligation on privacy by design and by default broadly equivalent to that of the GDPR, [68] which compels companies and organizations to set up technical and organizational measures in order for the data processing to meet the data protection rules. However, the Draft FDPA does not foresee any sanctions or penalties for a violation of these obligations (as opposed to the GDPR).

- The Draft FDPA includes a general obligation for companies to report to the Federal Data Protection and Information Commissioner ("FDPIC") as soon as possible (the data breaches which are likely to result in a high risk to the privacy or the fundamental rights of data subjects. [69] A notification of the data breach to data subjects may also be required if it is necessary for the protection of data subject or if such notification is ordered by the FDPIC. The Draft FDPA does not foresee a criminal sanctions for a violation of the obligation to notify data breaches, unless notification of data subjects is to be made based on an order from the FDPIC. The refusal to comply with the FDPIC's order may be criminally sanctioned with a fine up to CHF 250'000. [70]

- Under the Draft FDPA, it will no longer be the FDPIC who provides guidance on the adequacy level of third countries. The Draft FDPA delegates the qualification of adequacy to the Federal Council who will determine the countries providing for an adequate level of data protection. One may expect, however, that the Federal Council will follow closely the adoption of adequacy decisions by the European Commission.

- With regard to the authorities' investigations and fines, the Federal Data Protection FDPIC has the right to investigate on his own initiative or upon request, it may take investigation measures and is entitled to issue certain administrative measures. These investigation proceedings are governed by administrative procedural law, and are subject to review by the Federal Administrative Court. However, the FDPIC does not have the power to impose any fines or penalties. Instead, data protection violations lead to personal criminal liability of individuals, subject to fines of up to CHF 250,000 that will be imposed by the ordinary courts in Switzerland.

Until the Draft FDPA is finally enacted, the current FDPA of 19 June 1992 remains applicable. Initially, the Swiss Federal Council tentatively aimed to enact the Draft FDPA in August 2018. However, in January 2018, the relevant parliamentary commission required that the Draft FDPA be split in two parts to allow more time for deliberation.

For companies anticipating to be affected by both the Draft FDPA and the GDPR, it may be advisable to adjust all their processing of personal data to the standards provided under the GDPR. If the implementation and application of the Draft FDPA leads to certain obligations being leaner than those contained in the GDPR, these adjustments may be done in the course of the data processing activities (e.g., not applying the exercise of certain rights where these rights are not covered by the Draft FDPA and provided that the GDPR does not apply). To the extent that the Draft FDPA goes beyond the GDPR, the additional requirements should be implemented for any processing subject to the current FDPA respectively the Draft FDPA.

C. Turkey

Throughout 2018, the Turkish data protection authority (the "KVKK") has issued a number of regulations and guidance documents regarding a number of issues related to the application and enforcement of the Turkish Data Protection Act No. 6698 of 2016. These regulations and guidance documents include the following:

- Processing of sensitive personal data: On 7 March 2018, the KVKK published a decision regarding the processing of special categories of personal data. Pursuant to this decision, data controllers must foresee a separate policy and procedure for the protection of special categories of personal data. The decision further determined special conditions and requirements applicable to mediums where such data are stored, persons who have access to such data and transfer of such data.

- Transparency and information obligations: On 10 March 2018, the KVKK published the Communique on Procedures and Principles regarding the Obligation of Data Controllers to Inform, which lays out the content and methodology that shall be followed by entities and organizations to provide information to data subjects, for example within the scope of their privacy notices.

- Security measures: On 19 January 2018, the KVKK published a guidance document on security of personal data in order to assist entities and organizations in their compliance with data protection and security obligations, specifically focusing on technical and administrative measures. KVKK provided further detailed guidance on the matter with its decision on 31 January 2018 (2018/10).

- Registration of the data controllers: Pursuant to the KVKK Regulation on the Data Controller Registry, published on 30 December 2017, data controllers not exempted from registration by the KVKK must include their details in the KVKK Registry before proceeding to process personal data. Controllers may register online by uploading the required information to the KVKK Registry system. KVKK also declared the grace periods for different entities in its decision on 19 July 2018 (2018/88).

- Registration of e-marketing approvals and rejections: In 2018, Turkey adopted Law No. 7061 Amending Certain Tax Laws and Other Laws, which empowers the Ministry of Customs and Commerce to put in place a system to record the approvals and rejections received by companies for the purposes of e-marketing. This measure was later followed by a decision adopted by the KVKK, mandating all entities and organizations to cease their marketing operations unless they were covered by one of the exceptions provided for by the Turkish Data Protection Act or by consent.

- Data subject requests: On 10 March 2018, the KVKK also published the Communique on Procedures and Principles of Applications to Data Controllers, which lays out the procedure for data subjects to employ their rights against data controllers and data controllers' obligation with regards to such requests.

D. Ukraine

In Ukraine, on 23 October 2018, the Parliamentary Commissioner for Human Rights issued a draft law aiming to align the Law on Personal Data with the GDPR. The draft law was further updated on 30 October 2018, and is subject to additional revisions until it is finally filed by the Cabinet of Ministers to the Ukrainian Parliament. As it currently stands, the draft law contains the following main amendments:

- The draft sets out the legal basis upon which an entity may process personal data, including the consent, the performance of a contract to which the data subject is a party and the fulfilment of a legal obligation.

- The draft law borrows from the GDPR a number of principles and definitions, including the concepts of personal data, data processing, profiling and pseudonymisation.

- Like the GDPR, the draft law also regulates aspects such as the rights of data subjects, the appointment of DPOs, the notification of data breaches and the transfer of personal data to third countries and organizations.

In addition to the draft data protection law, on 9 May 2018, the Law on Basic Principles of Ukraine's Cyber Security came into force. The Cyber Security Law mainly applies to "critical infrastructure", and lays down the regulatory framework for a number of measures to be adopted in implementation of the Law.

III. Developments in Asia-Pacific

In an increasingly connected world, 2018 also saw many other countries try to get ahead of the challenges within the cybersecurity and data protection landscape. Several international developments bear brief mention here:

A. China

As noted in the 2018 International Outlook and Review, China's Cybersecurity Law was adopted on 1 June 2017, becoming the first comprehensive Chinese law to regulate the management and protection of digital information by companies. The law also imposes significant restrictions on the transfer of certain data outside of the mainland (data localization) enabling government access to such data before it is exported. [71]

Despite protests and petitions by governments and multinational companies, the implementation of the Cybersecurity Law continues to progress with the aim of regulating the behavior of many companies in protecting digital information. [72] While the stated objective is to protect personal information and individual privacy, and according to a government statement in China Daily, a state media outlet, to "effectively safeguard national cyberspace sovereignty and security," the law in effect gives the Chinese government unprecedented access to network data for essentially all companies in the business of information technology. [73] Notably, key components of the law disproportionately affect multinationals because the data localization requirement obligates international companies to store data domestically and undergo a security assessment by supervisory authorities for important data that needs to be exported out of China. Though the law imposes more stringent rules on critical information infrastructure operators (whose information could compromise national security or public welfare) in contrast to network operators (whose information capabilities could include virtually all businesses using modern technology), the law effectively subjects a majority of companies to government oversight. As a consequence, the reality for many foreign companies is that these requirements would likely be onerous, will increase the costs of doing business in China, and will heighten the risk of exposure to

industrial espionage. [74] Despite the release of additional draft guidelines meant to clarify certain provisions of the law, there is a general outlook that the law is still a work in progress, with the scope and definition still vague and uncertain. [75] Nonetheless, companies should endeavor to assess their data and information management operations to evaluate the risks of the expanding scope of the data protection law as well as their risk appetite for compliance with the Chinese government's access to their network data.

More recently, on 10 September 2018, the National People's Congress of China announced, as part of its legislative agenda, that its Standing Committee would consider draft laws with relatively mature conditions, including a draft personal information protection law and a draft data security law. [76]

B. Singapore

As indicated in the 2018 International Outlook and Review, the Personal Data Protection Commission of Singapore issued on 7 November 2017 the proposed advisory guidelines for the collection and use of national registration identification numbers. The guidance, which covers a great deal of personal and biometric data, emphasized the obligations of companies to ensure policies and practices are in place to meet the obligations for data protection under the Personal Data Protection Act of 2012. The Commission gives businesses and organizations 12 months from the date of publication to review their processes and implement necessary changes to ensure compliance. [77]

C. India

As noted in the 2018 International Outlook and Review, India recently issued a white paper in 2017 with the aim of drafting a data protection bill to "ensure growth of the digital economy while keeping personal data of citizens secure and protected". [78]

Further to the publication of this white paper, the Ministry of Electronics and Information Technology published, on 27 July 2018, the Personal Data Protection Bill (the “Bill”) and the Data Protection Committee Report (the “Report”). [79] The Bill comprises 15 chapters and addresses, data protection obligations, including, grounds for processing personal data and sensitive personal data, personal and sensitive data of children, data principal rights, transparency, accountability measures and transfer of personal data outside India. In particular, according to its Article 1, the Bill shall apply to the processing of personal data where such data has been collected, disclosed, shared or otherwise processes within the territory of India and to the processing of personal data by the State, any Indian company, any Indian citizen or any person or body of persons incorporated or created under Indian law. Notwithstanding the above, the Bill also applies to the processing of personal data by fiduciaries or data processors not present in the territory of India, if they carry out processing of personal data in connection with (i) any business carried on in India, (ii) systematic activity of offering goods or services to data principals within the territory of India, (iii) any activity which involves profiling of data principals within the territory of India.

Moreover, the Bill outlines that a data protection authority would be established and penalties would be imposed for violations of the obligations. In particular, Article 69(1) of the Bill establishes penalties that may extend up to five crore rupees (i.e., approx. USD 700,000; approx. EUR 620,000) or 2% of the data

fiduciary total worldwide turnover in the preceding financial year, whichever is higher, if the data fiduciary contravenes its obligations to take prompt and appropriate action in response to a data security breach, undertake a DPIA, conduct a data audit, appoint a DPO or if it fails to register within the relevant authority. In case the data fiduciary contravenes any of its obligations regarding the processing of personal and/or sensitive data, the need to adhere to security safeguards or the applicable provisions on transfer of personal data outside India, the Bill establishes a penalty that may extend up to 15 crore rupees or 4% of the data fiduciary total worldwide turnover in the preceding financial year, whichever is higher.

In addition, the Report addresses, among other things, existing approaches to data protection, key definitions of the Bill and recommendations received from the white paper consultation.

IV. Developments in Canada and in Latin America

The overhaul of data protection rules in important jurisdictions around the globe has also impacted Canada and Latin America, where some local administrations have bolstered their respective legislation and undertaken initiatives to bring their framework closer to that of the EU.

A. Brazil

In Brazil, a new General Data Protection Law was adopted on 14 August 2018 after several years of discussions among decision-makers. [80] Although the Brazilian Law is more lenient and contains fewer explanations regarding the interpretation and application of its provisions, a number of commonalities can be found between the Law and the GDPR, including the following:

- As the GDPR, the Brazilian General Data Protection Law generally excludes from its scope of application anonymous/ized data, except when the anonymization process used has been reverted, using solely its own resources, or where it can be reverted applying reasonable efforts. For this purpose, it is understood that anonymous/ized data is data that cannot be assigned to an identifiable person using reasonable means. [81]

- In setting out the obligations of entities processing personal data, the Brazilian General Data Protection Law also considers the conditions under which such processing is taking place. For example, while (as indicated above) anonymous/ised data may generally be considered to be excluded from the scope of application of the Law, it contains a specific provision whereby anonymous/ised data may fall within the scope of the Law if it is used to evaluate certain aspects of a physical person (e.g., the behavioral profile of a person if he/ she is identifiable). [82]

- The Brazilian Law is also based on the basic principle that data processing operations are forbidden unless they are based on any of its previously established legal basis. The Law contains 10 legal basis, which are based on the five legal basis contained in the GDPR, plus five additional basis: [83]

- data processing for the exercise of rights in legal proceedings;
- data processing for the research by study entities (granted that, whenever possible, the data is anonymous/ised);
- data processing for the protection of an individual's health;
- data processing for the protection to credit;
- data processing and sharing by the public administration as required for public policy enforcement under law or contract.

· In Brazil, consent is also defined as freely given, informed and unambiguous indication of data subjects' agreement to process personal data. Furthermore, the Law focuses on empowering data subjects with meaningful control and choice regarding their personal data. [84]

· As regards to the rights of data subjects, the Brazil Law has also included a general right to data portability, which was first envisaged by the GDPR. [85] This right obliges controllers to transfer personal data of data subjects to another controller, at the data subjects' request.

· The Law also contains a general obligation to report incidents regarding the processing of personal data to the national authority and to the data's subject, in a reasonable timeframe. The notification shall include information such as a description of the personal data affected and the data subjects and entities involved, a description of the technical and security measures used for the protection of personal data, the reasons for the delay suffered in the case of late notifications, and a description of the measures adopted to mitigate or redress the effects of the incident. [86]

· The Brazilian General Data Protection Law contains a general obligation to appoint a DPO, applicable to data controllers only. [87] However, the Brazilian data protection authority may set further guidance qualifying the situations where such obligation may no longer apply.

· Finally, as the GDPR, the Law prescribes the obligation to carry out a "Report on the Impact on Personal Data Protection" in certain situations, where a data processing operation may pose risks to civil liberties and fundamental rights.

· Like GDPR, the Brazilian General Data Protection Law provides that personal data can be transferred to third countries that ensure an adequate level of protection or based on appropriate safeguards. The safeguards under both laws are basically the same, except for legally binding instruments between public authorities/bodies, which is a safeguard under GDPR but under the Brazilian Law it is limited for purposes of international legal cooperation among intelligence, investigation and prosecution bodies (at least until the Brazilian data protection authority regulates the international transfer mechanisms).

- Fines under the Brazilian General Data Protection Law are capped at 2% of the turnover in Brazil in the preceding year or BRL 50 million (approximately USD 13 million), whichever is lower. These caps are applied to fines imposed per unlawful conduct.

- The Brazilian data protection authority was created on 28 December 2018, through Executive Order (MP) 869/2018, and will be composed of five commissioners, to be appointed by the President of the Republic, and advised by a National Council for the Protection of Personal Data and Privacy, composed of 23 unpaid members -- 11 members from different spheres of government and 12 members divided between four from the private sector, four from academia and four from the civil society. The Executive Order also postpones the entry into force of the Brazilian General Data Protection Law to August 2020.

B. Canada

As noted in the 2018 International Outlook and Review, Canada opened up for comments a proposed regulation in 2017 that would mandate reporting of privacy breaches under its Personal Information Protection and Electronic Documents Act of 2015 ("PIPEDA"). On 1 November 2018, some amendments to the PIPEDA came into force. [88] The law now establishes that, where an organization subject to PIPEDA experiences a data breach that gives rise to a "risk of significant harm", they will be required to: (i) report the incident to the Office of the Privacy Commissioner of Canada; (ii) notify any affected individuals; and (iii) alert any other third parties that are in a position to reduce the risk of harm to affected individuals.

C. Other Jurisdictions: Argentina, Chile, Colombia, Mexico, Panamá and Uruguay

Finally, as explained in the 2018 International Outlook and Review, **Argentina** forged ahead with an overhaul of the country's data protection regime by publishing in 2017 a draft data protection bill that would align the country's privacy laws with the GDPR requirements. [89] More recently, the Argentinian data protection authority announced, on 20 September 2018, that the President of the Argentine Republic, Mauricio Macri, had sent a draft data protection bill to the National Congress of Argentina for consideration, seeking to reform the current law on the protection of personal data. The message attached to the bill indicates that its objective is to modernize the law, in light of new technologies. The message attached to the bill also makes reference to the GDPR, and the bill includes provisions on data breach notification, privacy by design and default, processing of data by third parties, DPIA and the appointment of a DPO. [90]

In **Chile**, on 31 August 2018, the Superintendence of Banks and Financial Institutions announced that it had issued a series of modifications to Chapter 20-8 and 1-13 of the Updated Compilation of Standards relating to cybersecurity, including updates to the rules on the reporting of operational incidents. In particular, the modifications to Chapter 20-8 seek to improve the system for the reporting of security incidents by creating a digital platform, requiring incidents to be reported within 30 minutes of the incident occurring beginning 1 October 2018, and requiring entities to include specific information when reporting an incident. In addition, a number of obligations were also introduced, namely a requirement to appoint a person, at the executive level, to communicate with the Superintendence of Banks and

Financial Institutions (known as "SBIF", its acronym in Spanish); to inform users and clients of incidents that affect the quality and continuity of services, the security of their personal data or that are of public knowledge; and, to maintain a cybersecurity incident alert system to facilitate data sharing on the incidents in order to allow other entities to adopt any necessary measures. In relation to Chapter 1-13, the modifications establish cybersecurity as a special criteria in the evaluation of the management of a bank by the SBIF, and provides for a requirement to report on cybersecurity management at least once a year. In addition, the SBIF will also evaluate whether an entity maintains a cybersecurity incident database. [91]

Moreover, on 25 October 2018, the Chilean Transparency Council announced that the President of Chile, had changed the status of the draft data protection bill currently being considered by the National Congress of Chile to an urgent status. [92]

In **Colombia**, the Financial Superintendence of Colombia issued, on 5 June 2018, two circulars introducing requirements on cybersecurity risk management for covered entities, as well as security standards applicable to online payment platforms, in order to enhance the protection of consumers' personal financial information. In particular, the requirements include notifying consumers of cybersecurity incidents that affect the confidentiality or integrity of their information, as well as the measures adopted in response to incidents. With the publication of these circulars, entities will also be required to establish a unit in charge of cybersecurity risk management and a strategy concerning the sending of reports to supervisory authorities. In relation to online payment platforms, the security standards introduced are expected to enable the platforms, which are not regulated by the Financial Superintendence of Colombia, to offer their services to financial entities, such as banks and payment networks, under the supervision of this authority. [93]

Additionally, a legislative proposal seeking to modify and supplement the Statutory Law No. 1266 of 2008, concerning habeas data and financial information, has recently been presented to the Senate of the Republic of Colombia on 26 July 2018. [94]

In **Mexico**, the National Institute of Access to Information and Data Protection has been particularly active in 2018, issuing several guidance papers on several data protection topics. In March, the National Institute issued recommendations on the processing of the Mexican voting card (a widely used ID) by companies and public entities subject to the provisions of the Federal Law on the Protection of Personal Data Held by Private Parties 2010 and the General Law on the Protection of Personal Data Held by Public Entities 2017. [95] In May, the National Institute has issued guidance on biometric data, providing recommendations on how to process biometric data in compliance with the principles and obligations under the Federal Law on the Protection of Personal Data Held by Private Parties 2010 and the General Law on the Protection of Personal Data Held by Public Entities 2017 and clarifying when biometric data should be considered personal data. [96] In June, the National Institute issued guidance on how to manage data security incidents in order to assist companies, organizations and public entities to comply with their correspondent Data Protection Law . [97] In August, the National Institute issued guidance for the implementation of a "Data Protection Program" by those entities subject to the General Law on the Protection of Personal Data Held by Public Entities 2017. [98] Finally, in November, the National Institute issued guidance outlining the minimum criteria suggested for the contracting of cloud

computing services that involve the processing of personal data. The guide covers provider reputation and identity, minimum criteria to be considered by the customer to ensure that the provider has implemented security measures and has conducted risk assessment for personal data, the providers' return and destruction of personal data at the end of the service, and the conditions and practices of the provider regarding interoperability and portability. The guidance also includes checklists for companies and individuals subject to the Federal Law on the Protection of Personal Data Held by Private Parties 2010 to help them ensure compliance and analyze the risks they assume when hiring cloud computing products and services. [99]

Moreover, on 26 June 2018 Mexico acceded to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (known as "Convention 108") and its additional protocol.

In **Uruguay**, a bill on accountability and budget, containing provisions relating to data protection, is currently being analyzed by the Parliament of Uruguay. [100] Additionally, the data protection authority has recently issued, on 29 October 2018, data protection guides on cookies, profiling, bring your own device and drones, providing recommendations on their use in order to raise attention for data protection issues that may arise from the use of these technologies. [101]

---

[1] *See* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119 4.5.2016, p. 1.

[2] *See* Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, pp. 31-50.

[3] *See* GDPR, at Article 3.

[4] *See* EDPB, *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation* (16 November 2018), *available at* https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_en.pdf.

[5] *See* WP29, *Guidelines on Transparency under Regulation 2016/679* (WP260 rev.01, 11 April 2018), *available at* https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025.

[6] *See* WP29, *Guidelines on Consent under Regulation 2016/679* (WP259 rev.01; 10 April 2018), *available at* https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030.

[7] *See* GDPR, at Article 17.

[8] *See* EU Data Protection Directive, at Articles 12 and 14; and Case C-131/12 *Google Spain SL and Google Inc. v. AEPD and Mario Costeja González* ECLI:EU:C:2014:317.

[9] *See* WP29, *Guidelines on Personal Data Breach Notification under Regulation 2016/679* (WP250 rev.01; 6 February 2018), *available at* https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49827.

[10] *See* WP29, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (WP251 rev.01; 6 February 2018), *available at* https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826.

[11] *See* GDPR, at Article 35.

[12] *See* WP29, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (WP248 rev.01; 4 October 2017), *available at* http://ec.europa.eu/newsroom/document.cfm?doc_id=47711.

[13] *See* WP29, *Guidelines on the right to data portability* (WP242 rev.01; 5 April 2017), *available at* http://ec.europa.eu/newsroom/document.cfm?doc_id=44099.

[14] *See* GDPR, at Article 56(2).

[15] *See* GDPR, at Article 56(1).

[16] *See* GDPR, at Article 63.

[17] *See* GDPR, at Article 66.

[18] *See* WP29, *Guidelines for Identifying a Controller or Processor's Lead Supervisory Authority* (WP244 rev.01; 5 April 2017), *available at* http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

[19] *See* WP29, *Guidelines on Data Protection Officers ("DPOs")* (WP243 rev.01; 5 April 2017), *available at* http://ec.europa.eu/newsroom/document.cfm?doc_id=44100.

[20] *See*: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en.

[21] The Investigation Update "*Investigation into the use of data analytics in political campaigns*", 11.07.2018 is *available at* https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf.

[22] The notice is *available at* https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf.

[25] The press release is *available at* http://news.marriott.com/2019/01/marriott-provides-update-on-starwood-database-security-incident/.

[26] For more information, the press release is *available at* https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc

[27] For more information, the decision is *available at* https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000038032552&fastReqId=2103387945&fastPos=1.

[28] For more information, the press release is *available at* https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-opens-statutory-inquiry-twitter.

[29] *See*: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.

[30] *See* European Commission, "EU and Japan sign Economic Partnership Agreement" (17 July 2018), *available at* http://europa.eu/rapid/press-release_IP-18-4526_en.htm.

[31] *See*: http://europa.eu/rapid/press-release_IP-18-5433_en.htm.

[32] *See* EDPB, Opinion 28/2018 regarding the European Commission Draft Implementing Decision on the adequate protection of personal data in Japan (5 December 2018), *available at* https://edpb.europa.eu/sites/edpb/files/files/file1/2018-12-05-opinion_2018-28_art.70_japan_adequacy_en.pdf.

[33] *See* IAPP, "South Korea's EU adequacy decision rests on new legislative proposals" (27 November 2018), *available at* https://iapp.org/news/a/south-koreas-eu-adequacy-decision-rests-on-new-legislative-proposals/.

[34] *See* Irish High Court Commercial, *The Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems*, 2016 No. 4809 P.

[35] *See* CJEU, Case C-362/14, *Maximillian Schrems v. Data Protection Commissioner* (6 October 2016).

[36] *See* CJEU, Case C-293/12, *Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources et al* (8 April 2014).

[37] *See* European Parliament, Adequacy of the protection afforded by the EU-US Privacy Shield (5 July 2018), *available at* http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2018-0315&format=XML&language=EN.

[38] *See* European Commission, "Joint Press Statement from Commissioner Věra Jourová and Secretary of Commerce Wilbur Ross on the Second Annual EU-U.S. Privacy Shield Review" (19 October 2018), *available at* http://europa.eu/rapid/press-release_STATEMENT-18-6157_en.htm.

[39] *See* Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, pp. 1-30, *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC.

[40] *E.g.*, domain name systems (DNS) providers and top level domain (TLD) registries; *see* Article 4, NIS Directive.

[41] *See* NIS Directive, at Article 7.

[42] *See* NIS Directive, at Recital (57) and Article 3.

[43] *See* NIS Directive, at Article 16(10).

[44] *See* NIS Directive, at Articles 16(8) and (9).

[45] *See* ENISA, "Guidelines on assessing DSP security and OES compliance with the NISD security requirements" (28 November 2018), *available at* https://www.enisa.europa.eu/publications/guidelines-on-assessing-dsp-security-and-oes-compliance-with-the-nisd-security-requirements.

[46] *See* ENISA, "Guideline on assessing security measures in the context of Article 3(3) of the Open Internet regulation" (12 December 2018), *available at* https://www.enisa.europa.eu/publications/guideline-on-assessing-security-measures-in-the-context-of-article-3-3-of-the-open-internet-regulation.

[47] *See* https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot.

[48] *See* https://www.enisa.europa.eu/publications/towards-secure-convergence-of-cloud-and-iot

[49] *See* ENISA, "Cyber Eurrope 2018: After Action Report" (December 2018), *available at* https://www.enisa.europa.eu/publications/cyber-europe-2018-after-action-report/at_download/fullReport.

[50] *See* https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation.

[51] *See* http://ec.europa.eu/newsroom/document.cfm?doc_id=44103.

[52] *See* http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A8-2017-0324& language=EN.

[53] *See* draft ePrivacy Regulation, at Recital (13). *See* Explanatory Memorandum, at Section 3.2.

[54] *See* draft ePrivacy Regulation, at Article 8(1).

[55] However, in practice, the WP29 had already expressed the possibility that operators do not obtain consent for the setting and receipt of cookies in some of the circumstances now covered in the draft ePrivacy Regulation, provided that certain conditions are met. *See* WP29, *Opinion 04/2012 on Cookie*

Consent Exemption (WP 194; 7 June 2012), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf.

[56] *See* draft ePrivacy Regulation, at Articles 18 ff.

[57] *See* WP29, *Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)* (WP247; 4 April 2017), *available at* http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

[58] *See* European Parliament's proposal, *available at* http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A8-2017-0324& language=EN.

[59] *See*: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_10975_2018_INIT&from=EN.

[60] *See* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_13256_2018_INIT&from=EN.

[61] *See* CJEU, Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH* (5 June 2018).

[62] *See* Opinion of Advocate General Bobek on Case C-498/16 *Maximilian Schrems v. Facebook Ireland Limited*.

[63] The Draft FDPA is available in the official languages of Switzerland:

- French: https://www.ejpd.admin.ch/ejpd/fr/home/aktuell/news/2017/2017-09-150.html
- German: https://www.ejpd.admin.ch/ejpd/de/home/aktuell/news/2017/2017-09-150.html
- Italian: https://www.ejpd.admin.ch/ejpd/it/home/aktuell/news/2017/2017-09-150.html

An unofficial English version of the Draft FDPA is also available at https://www.dataprotection.ch/fileadmin/dataprotection.ch/user_upload/redaktion/Docs/Swiss_Data_Protection_Act__draft_of_September_2017__Walder_Wyss_convenience_translation_V010.pdf?v=1507206202

[64] *See* Draft FDPA, Article 4(b). Please note that the current FDPA protects information relating to legal entities as personal data.

[65] *See* Draft FDPA, Articles 5(1) to (5).

[66] *See* Draft FDPA, Articles 19 and 23 to 28.

[67] *See* Draft FDPA, Article 20.

[68] *See* Draft FDPA, Article 6, and GDPR, Article 25.

[69] *See* Draft FDPA, Article 22.

[70] *See* Draft FDPA, Article 57.

[71] *See* FT Cyber Security, "China's cyber security law rattles multinationals," *Financial Times* (30 May 2017), *available at* https://www.ft.com/content/b302269c-44ff-11e7-8519-9f94ee97d996.

[72] *See* Alex Lawson, "US Asks China Not To Implement Cybersecurity Law," Law360 (27 September 2017) *available at* https://www.law360.com/articles/968132/us-asks-china-not-to-implement-cybersecurity-law.

[73] *See* Sophie Yan, "China's new cybersecurity law takes effect today, and many are confused," CNBC.com (1 June 2017), *available at* https://www.cnbc.com/2017/05/31/chinas-new-cybersecurity-law-takes-effect-today.html.

[74] *See* Christina Larson, Keith Zhai, and Lulu Yilun Chen, "Foreign Firms Fret as China Implements New Cybersecurity Law", Bloomberg News (24 May 2017), *available at* https://www.bloomberg.com/news/articles/2017-05-24/foreign-firms-fret-as-china-implements-new-cybersecurity-law.

[75] *See* Clarice Yue, Michelle Chan, Sven-Michael Werner and John Shi, "China Cybersecurity Law update: Draft Guidelines on Security Assessment for Data Export Revised!," *Lexology* (26 September, 2017), *available at* https://www.lexology.com/library/detail.aspx?g=94d24110-4487-4b28-bfa5-4fa98d78a105.

[76] *See* http://www.npc.gov.cn/npc/xinwen/2018-09/10/content_2061041.htm (Press Release in Chinese).

[77] *See* Singapore Personal Data Protection Commission, Proposed Advisory Guidelines on the Personal Data Protection Act For NRIC Numbers, published 7 November 2017, *available at* https://www.pdpc.gov.sg/docs/default-source/public-consultation-6---nric/proposed-nric-advisory-guidelines---071117.pdf?sfvrsn=4.

[78] *See* Naïm Alexandre Antaki and Wendy J. Wagner, "No escaping notification: Government releases proposed regulations for federal data breach reporting & notification", *Lexology* (6 September 2017), *available at* https://www.lexology.com/library/detail.aspx?g=0a98fd33-1f2c-4a52-98c0-cf1feeaf0b90; Ministry of Electronics & Information Technology, "White Paper of the Committee of Experts on a Data Protection Framework for India," Government of India (27 November 2017), *available at* http://meity.gov.in/white-paper-data-protection-framework-india-public-comments-invited.

[79] *See* http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdf

[80] *See* IAPP, "GDPR matchup: Brazil's General Data Protection Law" (4 October 2018), *available at* https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/.

[81] *See* Brazilian General Data Protection Law, Article 12.

[82] *See* Brazilian General Data Protection Law, Article 12.

[83] *See* Brazilian General Data Protection Law, Article 7.

[84] *See* Brazilian General Data Protection Law, Article 7.

[85] In Brazil, under local telecommunications regulations, users could request the portability of personal data related to a telephone number (Resolution 460/07 of the Brazilian National Telecommunications Agency, Anatel), *available at* http://www.anatel.gov.br/legislacao/resolucoes/22-2007/8-resolucao-460.

[86] *See* Brazilian General Data Protection Law, Article 48.

[87] *See* Brazilian General Data Protection Law, Article 41.

[88] These amendments were implemented through the Digital Privacy Law of 2015, *available at* https://www.canlii.org/en/ca/laws/astat/sc-2015-c-32/121166/sc-2015-c-32.html.

[89] *See* Office of the Australian Information Commissioner, "De-identification Decision-Making Framework", Australian Government (18 September 2017), *available at* https://www.oaic.gov.au/agencies-and-organisations/guides/de-identification-decision-making-framework; Lyn Nicholson, "Regulator issues new guidance on de-identification and implications for big data usage", *Lexology* (26 September 2017) *available at* https://www.lexology.com/library/detail.aspx?g=f6c055f4-cc82-462a-9b25-ec7edc947354; "New Regulation on the Deletion, Destruction or Anonymization of Personal Data," British Chamber of Commerce of Turkey (28 September 28, 2017), *available at* https://www.bcct.org.tr/news/new-regulation-deletion-destruction-anonymization-personal-data-2/64027; Jena M. Valdetero and David Chen, "Big Changes May Be Coming to Argentina's Data Protection Laws," *Lexology* (5 June 2017), *available at* https://www.lexology.com/library/detail.aspx?g=6a4799ec-2f55-4d51-96bd-3d6d8c04abd2.

[90] *See* https://www.argentina.gob.ar/noticias/proteccion-de-datos-personales-al-congreso (press release only available in Spanish).

[91] *See* https://www.sbif.cl/sbifweb/servlet/Noticia?indice=2.1&idContenido=12214 (press release only available in Spanish).

[92] *See* https://www.consejotransparencia.cl/presidente-del-cplt-asegura-estar-cada-vez-mas-cerca-el-fin-del-abuso-tras-anuncio-de-urgencia-al-proyecto-de-proteccion-de-datos-personales/ (press release only available in Spanish).

[93] *See* the press release of 5 June 2018, *available at* https://www.superfinanciera.gov.co/inicio/sala-de-prensa/comunicados-de-prensa-/comunicados-de-prensa--10082460 (press release only available in Spanish).

[94] *See* http://leyes.senado.gov.co/proyectos/images/documentos/Textos%20Radicados/proyectos%20de%20ley/2018%20-%202019/PL%20053-18%20Habeas%20Data.pdf

[95] The guide is *available at* http://inicio.inai.org.mx/DocumentosdeInteres/RecomendacionesCredencialV.pdf

[96] The guide is *available at* http://inicio.ifai.org.mx/DocumentosdeInteres/GuiaDatosBiometricos_Web_Links.pdf

[97] The guide is *available at* http://inicio.inai.org.mx/DocumentosdeInteres/Recomendaciones_Manejo_IS_DP.pdf

[98] The guide is *available at* http://inicio.inai.org.mx/DocumentosdeInteres/DocumentoOrientadorPPDP.docx

[99] The guide is *available at* http://inicio.ifai.org.mx/nuevo/ComputoEnLaNube.pdf

[100] The draft bill is *available at* https://www.mef.gub.uy/innovaportal/file/24846/1/fundamentacion-del-articulado.pdf.

[101] *See* https://www.datospersonales.gub.uy/inicio/institucional/noticias/urcdp_lanzo_nuevas_guias_proteccion_datos_personales (press release only available in Spanish).

The following Gibson Dunn lawyers assisted in the preparation of this client alert: Ahmed Baladi, Alexander Southwell, Alejandro Guerrero, Clémence Pugnet and Francisca Couto.

Gibson Dunn's lawyers are available to assist with any questions you may have regarding these issues. For further information, please contact the Gibson Dunn lawyer with whom you usually work or any of the following leaders and members 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)207071 4250, jacox@gibsondunn.com)
Patrick Doris - London (+44 (0)20 7071 4276, pdoris@gibsondunn.com)

Penny Madden - London (+44 (0)20 7071 4226, pmadden@gibsondunn.com)
Jean-Philippe Robé - Paris (+33 (0)1 56 43 13 00, jrobe@gibsondunn.com)
Michael Walther - Munich (+49 89 189 33-180, mwalther@gibsondunn.com)
Kai Gesing - Munich (+49 89 189 33-180, kgesing@gibsondunn.com)
Sarah Wazen - London (+44 (0)20 7071 4203, swazen@gibsondunn.com)
Vera Lukic - Paris (+33 (0)1 56 43 13 00, vlukic@gibsondunn.com)
Alejandro Guerrero - Brussels (+32 2 554 7218, aguerrero@gibsondunn.com)

Asia
Kelly Austin - Hong Kong (+852 2214 3788, kaustin@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)
M. Sean Royall - Dallas (+1 214-698-3256, sroyall@gibsondunn.com)
Debra Wong Yang - Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)
Ryan T. Bergsieker - Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)
Richard H. Cunningham - Denver (+1 303-298-5752, rhcunningham@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)
Shaalu Mehra - Palo Alto (+1 650-849-5282, smehra@gibsondunn.com)
Karl G. Nelson - Dallas (+1 214-698-3203, knelson@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)

Questions about SEC disclosure issues concerning data privacy and cybersecurity can also be addressed to the following leaders and members of the Securities Regulation and Corporate Governance Group:

James J. Moloney - Orange County, CA (+1 949-451-4343, jmoloney@gibsondunn.com)
Elizabeth Ising - Washington, D.C. (+1 202-955-8287, eising@gibsondunn.com)
Lori Zyskowski - New York (+1 212-351-2309, lzyskowski@gibsondunn.com)