GIBSON DUNN

January 29, 2020

INTERNATIONAL CYBERSECURITY AND DATA PRIVACY OUTLOOK AND REVIEW – 2020

To Our Clients and Friends:

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

Like many recent years, 2019 saw significant developments in the evolution of the data protection and cybersecurity landscape in the European Union ("**EU**"):

- Several EU Member States continued to adapt their national legal frameworks, and data protection authorities started to apply and enforce these laws and the GDPR.

- The Court of Justice of the EU ("**CJEU**") has started to hear cases and delivered rulings that concern the application of the General Data Protection Regulation ("**GDPR**")[1] and EU data privacy legislation. The European Data Protection Board ("**EDPB**"), the EU's regulatory body that took office in 2018 and is composed by representatives of all EU data protection authorities, continued to adopt relevant opinions and guidance documents regarding the interpretation of the GDPR.

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

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

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

Table of Contents

I. European Union

A. EU GDPR: Implementation Application and Enforcement

As is widely known, in 2018 the GDPR became the main legislative act for the protection of personal data and privacy in the EU. Its numerous and lengthy provisions have made the object of interpretation on their application and enforcement by the CJEU and by the EU data protection authorities gathered in the EDPB.[2]

1. National Data Protection Initiatives Implementing and Applying the GDPR

Since the adoption of the GDPR, some Member States have adapted their legal frameworks in order to transpose and implement some of the GDPR provisions into their respective national legislation.

In the 2019 International Outlook and Review, we provided an overview of the national laws and regulations adopted by the Member States in 2018 in order to adapt their legislation to the GDPR.

Below is an overview of the national data protection reforms implemented throughout the EU during 2019:

Member State	National Data Protection Law Adopted
Bulgaria	Personal Data Protection Act of 4 January 2002 implementing the GDPR, published in the State Gazette on 26 February 2019.
Czech Republic	Act No. 110/2019 Coll. on the Processing of Personal Data (Data Protection Act), applicable as of its publication in the Official Gazette on 24 April 2019.
Finland	Data Protection Act (1050/2018), approved on 13 November 2018 and applicable as of 1 January 2019.
France	Decree No. 2019-536 of 29 May 2019.
Germany	Second Law on the Adaptation of Data Protection Legislation to the GDPR, published in the Federal Gazette on 25 November 2019.

Member State	National Data Protection Law Adopted
Greece	Law 4624/2019 on the protection of personal data of 29 August 2019.
Poland	Act of 21 February 2019 amending other legal acts in relation to the implementation of the GDPR.
Portugal	Law No. 58/2019 of 8 August 2019, which repealed the previous data protection law, Law No. 67/98, of 26 October 1998.
Romania	Law no. 129 of 15 June 2018 amending the Law No. 102 of 2005.
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"). On 6 March 2019, the Ministry of Justice released a draft Personal Data Protection Act.

2. GDPR Cases, Investigations and Enforcement

2019 saw the end of the transition period that supervisory authorities granted to companies to implement the GDPR, and investigations and infringement proceedings have sky-rocketed in the Member States. The most significant cases in important EU jurisdictions are set out below.

In **France,** the French National Data Protection Commission ("**CNIL**") received group complaints from the associations None Of Your Business and La Quadrature du Net in May 2018, shortly after the application of the GDPR. 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. The CNIL concluded that Google had breached its transparency and information obligations and its obligation to rely on a valid legal basis to customize and deliver personalized ads. Based on these grounds, the CNIL imposed a financial penalty of EUR 50 million to Google LLC on 21 January 2019.[3]

The CNIL has also imposed a 500,000 EUR fine on a company specialized in private homes insulation, Futura Internationale, for violations of the GDPR. Further to a complaint, the CNIL investigated and found Futura Internationale to have committed the following GDPR violations: (i) the absence of a procedure to ensure the right of data subjects to object to personal data processing; (ii) the presence of irrelevant data in the company's client database (e.g., offensive comments and comments related to health); (iii) insufficient information provided to individuals regarding the processing of their personal data and their rights; (iv) lack of cooperation with the CNIL; and (v) lack of mechanisms of supervision and compliance of data transfers outside the EU.

In **Ireland**, a social network 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 in public messages. The company refused to disclose the data it recorded when a user clicked on links in other people's messages, claiming that it benefitted from a GDPR exemption to disclose the requested data, as providing it would involve a "disproportionate effort" for the company.

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.[4] In 2019, the Irish Data Protection Commission concluded its investigation into the social network service over potential violations of the GDPR, and moved into the decision-making phase. During this phase, the Irish Data Protection Commission will issue a draft decision, which is expected in early 2020.

On another note, in **Germany**, the Berlin Commissioner for Data Protection and Freedom of Information imposed a fine of approximately 14.5 million EUR on a German real estate company for violations of the privacy by design and storage-limitation principles. In particular, the Berlin authority found that the archive system of the company did not enable personal data that were no longer required to be removed, and personal data were retained for longer than necessary.[5] This is the highest fine imposed so far by a German company over data protection.

The German Federal Data Protection Supervisory Authority also imposed a 9.55 million EUR fine on a telecommunications service provider for violations of the GDPR. The authority concluded that individuals calling the provider's customer service hotline could obtain, merely by providing a customer's name and date of birth, extensive information about other customers. The authority considered that this constituted a breach of Article 32 of the GDPR, which requires data controllers to implement technical and organizational measures to ensure a level of security appropriate to risks.[6] The company announced that it would challenge the order, arguing that the amount of the fine is disproportionate.

In the **UK**, on 9 July 2019, the Information Commissioner Office ("**ICO**") issued a notice of its intention to fine a hospitality company approximately 99 million GBP for infringements of the GDPR. The proposed fine relates to an incident that affected personal data contained in approximately 30 million guest records of residents in the European Economic Area.[7] The cyber-incident and possible data breach affected the company while it was subject to one ownership, but the breach was exposed and investigated after the company was transferred to another ownership.

On 8 July 2019, the ICO also issued a notice of its intention to fine British Airways 183.39 million GBP for infringements of the GDPR. The proposed fine relates to a cyber-incident reported to the ICO by British Airways in September 2018, according to which personal data of approximately 500,000 customers were compromised.[8]

On 17 December 2019, the ICO imposed a fine of 275,000 GBP, the first issued in the UK in application of the GDPR, on a pharmacy for failing to comply with security requirements for special categories of data. The pharmacy allegedly left approximately 500,000 documents (containing clients' personal data

including names, addresses, dates of birth, National Health Service numbers, as well as other medical information) in unlocked containers at the back of its premises. The ICO was alerted to this incident by the Medicines and Healthcare Products Regulatory Agency, which was carrying out its own separate investigation into the pharmacy. After completing its investigation, the ICO concluded that the pharmacy failed to process data in a manner that ensured appropriate security against unauthorized or unlawful processing and accidental loss, destruction or damage, in violation of the GDPR.[9]

In **Austria**, the Austrian data protection authority imposed a fine of 18 million EUR on the Austrian Postal Service, due to the processing of personal data on political opinions of data subjects and for direct marketing purposes. The authority specified that the high amount of the fine imposed on the Austrian Postal Service aimed to prevent other violations.[10]

Finally, in **Italy**, the Italian data protection authority recently imposed a fine of 11.5 million EUR on energy company Eni Gas and Luce for its unlawful processing of personal data in the context of promotional activities (telemarketing) and the activation of unsolicited contracts. The fines were determined in line with the GDPR requirements, taking into account the wide range of stakeholders involved, the pervasiveness of the conduct, the duration of the infringement, and the economic conditions of the company.[11]

3. CJEU Case Law

Building on the body of case law developed throughout the last years, as we indicated in the 2019 International Outlook and Review, 2019 has continued to witness numerous cases before the CJEU on the application of the EU Data Protection Directive, the GDPR and the ePrivacy Directive. Set forth below are the most relevant cases and updates concerning the interpretation and application of EU privacy legislation.

a) Territorial Scope of the "Right To Be Forgotten" under the GDPR

On 24 September 2019, the CJEU delivered a judgment in a case facing Google LLC to the French supervisory authority ("**CNIL**"). In the underlying proceedings under French law, Google LLC had a fine imposed for its failure to implement on all domain extensions, worldwide, those requests from data subjects to remove search results that referenced their personal data. The CNIL considered it insufficient that "right to be forgotten" requests from French data subjects would only be executed in results on the ".fr" domain of Google Search (i.e., www.google.fr), as well as only with regard to users located within the French territory.[12]

In its judgment, the CJEU concluded that a search engine operator is not required to carry out that de-referencing on all versions of its search engine, but only on the versions of that search engine corresponding to all the EU Member States.

b) Cookie Consent under the ePrivacy Directive

On 1 October 2019, the CJEU issued a ruling on the topic of cookie information and consent obligations under the ePrivacy Directive and under the GDPR. The judgment was delivered in the context of

proceedings followed in Germany against Planet49 GmbH, a company that organized a promotional lottery online and which required users to input certain personal data in order to participate, followed by pre-selected checkboxes authorizing Planet49 GmbH to share the personal data with analytics providers, sponsors and cooperation partners for commercial purposes.[13]

In the judgment, the CJEU considered that the "consent" referred to in the ePrivacy Directive, which is based on the definition provided in the GDPR, is not valid if it is collected by way of pre-selected checkboxes, which the user must deselect in order to refuse his or her consent. Accordingly, in the context of the use of checkboxes, valid "consent" may only be expressed through the use of blank boxes that users must actively select.

The ruling applies in principle to the processing of data contained in cookies, stored and accessed in users' devices, regardless of whether these data may be considered to be personal data. However, given that the CJEU expressly referred to and based its decision on the definition of "consent" under the GDPR, it is possible that this ruling will set a new trend in the definition of "consent" applicable to the processing of personal data in general.

Furthermore, the CJEU ruled that online service providers must make available to website users information on the operation of cookies, including the duration of the operation of cookies and whether or not third parties may have access to any cookie data received.

c) Obligations of Website Providers and Social Network Services Offering Social Plug-ins

On 29 July 2019, the CJEU delivered a judgment regarding the identification of controllers and defining the scope of information obligations imposed on online service providers. The ruling was issued in the proceedings followed against Fashion ID, an online clothing retailer, which had embedded in its website a "Like" social plug-in from a third-party social network service. Because of the manner in which the Internet works, when a visitor consulted the website of Fashion ID, that visitor's personal data (e.g., IP addresses, cookie data and other browser technical data) were transmitted to the social network service through the social plug-in. Such transmission occurred without the knowledge or awareness of the visitor, and independently from the visitor's membership with the social network.[14]

In the judgment, the CJEU concluded that the operator of a website, such as Fashion ID, which embeds in its website a social plug-in that transmits personal data to a third-party provider, can be considered to be a "controller." However, the CJEU limited the role of Fashion ID as a "controller" only for the purposes of those data processing operations in respect of which it actually determined the purposes and means.

Furthermore, the CJEU found that both the provider of the website (Fashion ID) and of the social plug-in (the social network service provider) should each pursue a legitimate interest in order to benefit from the legal basis provided for in Article 7(f) of Directive 95/46/EC (Article 6(1)(f) of the GDPR).

Finally, the CJEU concluded that the website provider (Fashion ID) needed to obtain any valid consent required, and needed to provide users with the necessary information to comply with Directive 95/46/EC

(replaced by the GDPR), but only with regard to the data processing operations in respect of which the provider determined the purposes and means as a "controller."

d) Validity of Data Transfer Mechanisms: Standard Contract Clauses and the EU-U.S. Privacy Shield

As it was indicated in the 2018 and 2019 International Outlook and Review, on 3 October 2017, the Irish High Court decided to refer the issue of the validity of the standard contractual clauses decisions to the CJEU for a preliminary ruling.[15] Several questions were referred to the Court in May 2018 which relate, in particular, to the validity of Decision 2010/87 on standard contractual clauses ("**SCCs**") for the transfer of personal data to processors established in third countries. On 19 December 2019, the EU Advocate General issued a favorable opinion on the validity of the EU's SCCs.[16]

According to the Advocate General, Decision 2010/87 is compatible with the Charter of Fundamental Rights of the EU since there are sufficiently sound mechanisms to ensure that transfers based on the SCCs be suspended or prohibited where those clauses are breached or impossible to honor. Decision 2010/87 places obligations on data controllers and, where the latter fail to act, on EU data protection authorities, to suspend or prohibit a transfer when, because of a conflict between the obligations arising under the standard clauses and those imposed by the law of the third country of destination, those clauses cannot be complied with.[17] The final judgment of the CJEU should be adopted and released in the coming months.

As it was also indicated in the 2018 and 2019 International Outlook and Review, on 12 July 2016, the European Commission formally approved the EU-U.S. Privacy Shield. The Privacy Shield replaced the EU-U.S. Safe Harbor framework for the transatlantic transfer of personal data, which was invalidated by the CJEU on 6 October 2015 in the case *Maximilian Schrems v. Data Protection Commissioner*.[18] Since the adoption of the Privacy Shield program in 2016, more than 5,000 companies have adhered to the Privacy Shield framework.

On 22 November 2017, the CJEU declared an action brought by Digital Rights Ireland Ltd. against the Privacy Shield inadmissible. However, the EU's General Court admitted a similar challenge of the Privacy Shield brought by French NGO *La Quadrature du Net*.[19] These proceedings are currently ongoing, and an opinion of the EU's Advocate General and a Judgment are expected in the course of 2020.

In October 2019 the European Commission published its third annual review of the EU-U.S. Privacy Shield, which concluded that the Privacy Shield continues to ensure an adequate level of protection of personal data transferred to participating companies in the U.S.[20] The European Commission noted the adoption of several improvements to the Privacy Shield, such as a more systematic oversight performed by the U.S. Department of Commerce, an improvement of the enforcement action by the Federal Trade Commission, the use of Privacy Shield rights by an increasing number of European individuals, or the appointment of the permanent Ombudsperson. Nevertheless, the European Commission recommended the adoption of additional measures to ensure the effective functioning of the Privacy Shield, including the strengthening of the certification/recertification process, the

development of additional guidance related to human resources data, and the expansion of compliance checks.

On 12 November 2019, the EDPB published its own report relating to this third annual review, which contains its main findings regarding the commercial aspects of the Privacy Shield and the access by public authorities to data transferred from the EU to the U.S. under the Privacy Shield.[21]

4. Guidance Adopted by the EDPB

The EDPB, which took office on 25 May 2018, has continued to hold public consultations and adopt Guidelines on the interpretation and application of certain key provisions and aspects of the GDPR. The Guidelines adopted in the course of 2019 include the following:[22]

- GDPR applicability: Guidelines 3/2018 on the territorial scope of the GDPR (Article 3

  These Guidelines analyze the different elements that determine whether an entity is subject to the GDPR, depending on whether or not it has an establishment in the EU. Remarkably, the EDPB clarified in the Guidelines that controllers or processors not established in the EU could be subject to the GDPR if they *intentionally* target EU data subjects to offer goods or services, or if they monitor their behavior. Furthermore, these foreign entities would not benefit from the "one-stop shop" rule if they do not have one or more establishments in the EU.

- Processing on the basis of the performance of the contract: Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects.

  These Guidelines assess the application of the legal basis contained in Article 6(1)(b) of the GDPR, which may be relied upon when personal data are processed for the performance of a contract with a data subject or in order to take steps at the request of the data subject prior to entering into a contract. In particular, the EDPB found that Article 6(1)(b) of the GDPR may not cover certain processing activities not necessary for the provision of individual services requested by a data subject, but rather for the controller's wider business model.

- Right to be forgotten: Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1).

  In these Guidelines, the EDPB has dissected each of the grounds that data subjects may rely on to exercise their right to be forgotten, and the exceptions on which data controllers may rely on to dismiss this kind of requests, including the necessity to safeguard the right of freedom of expression and information.

- Privacy-friendly techniques and practices: Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.

  The EDPB issued these Guidelines in order to shed some light into one of the most unclear

obligations imposed by the GDPR. The EDPB clarified that privacy "by design and by default" required companies to implement necessary and effective safeguards in the form of technical and organizational measures. These should include state-of-the-art technology considered appropriate regarding the costs of implementation, the nature, scope, context and purpose of the processing, and the risks identified at the time of the processing.

- Processing of personal data through video devices: Guidelines 3/2019 on processing of personal data through video devices.

  In these long-awaited Guidelines, the EDPB expressed a common EU approach to the use of video devices (e.g., CCTV cameras) and the processing of personal data. The EDPB analyzed the possible application of a number of legal bases (e.g., consent, legitimate interests, or performance of a task in the public interest) and assessed the application of the data protection principles to video footage recording (e.g., technical and organizational measures, storage periods). It also addressed the conditions for the disclosure of video footage to third parties, and the exercise of rights by data subjects.

- Certification bodies and criteria:

  Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679).

  Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679.

The GDPR foresees the appointment of accredited bodies that can certify the compliance of companies and organizations with data protection rules. In these Guidelines, the EDPB outlined the procedure for the accreditation of these certification bodies, and set out the substantive requirements for certification of entities' compliance with the substantive requirements of the GDPR.

- Codes of conduct: Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679.

  Under the GDPR, trade associations and other institutional bodies representing controllers or processors may prepare codes of conduct for the purposes of specifying the application of the GDPR in specific fields. These Guidelines provided the criteria for the admissibility and approval of codes, including at the national and EU level, and set up a procedure for their monitoring by accredited bodies, approval and revocation.

5. International Transfers: Adequacy Declarations and Challenges

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 where personal data is being transferred protects personal data adequately.

Thus far, the adequacy decisions adopted by the European Commission under the previous legal framework (the Data Protection Directive 95/46/EC) are still in force, and cover data transfers to the following jurisdictions: Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the U.S. (limited to the EU-U.S. Privacy Shield framework).[23]

As indicated in the 2019 International Outlook and Review, the European Commission had engaged with a number of jurisdictions with a view to recognizing the validity of data transfers to more countries worldwide.

During 2019, adequacy talks have continued with regard to South Korea, with a view to adopting an adequacy decision in 2020. Although the negotiations have remained confidential so far, it has been reported that the main concerns of the EU authorities related to the independence and powers of the South Korean data protection authority.[24] Some amendments to the Personal Information Protection Act have been submitted to the South Korean National Assembly, in order to grant enforcement power and functions to the Personal Information Protection Commission.

India, which is preparing a personal data protection bill, would also plan to obtain an adequacy decision following the finalization and adoption of this bill.[25] In addition, the evolution of the situation in Indonesia and Taiwan could also lead to future adequacy decisions. Finally, preparatory work has started in order to initiate discussions regarding the adequacy of several Latin American countries (such as Chile or Brazil).[26]

B. EU Cybersecurity Directive ("NIS Directive")

In the EU, cybersecurity legislation addressing incidents affecting essential service and digital service providers is primarily covered by the NIS Directive,[27] adopted on 6 July 2016. As it was explained in the 2019 International Outlook and Review, the NIS Directive is the first set of cybersecurity rules to be adopted at the EU level, which aims to set a minimum level of cybersecurity standards and to streamline cooperation between EU Member States at a time of growing cybersecurity breaches.

In the course of 2019, the European Union Agency for Cybersecurity ("**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 GDPR[28] and the NIS Directive.[29]

- Following the trends for increased use of consumer products and services relying on cloud services and Internet of Things, ENISA has continued to issue guidance documents providing companies with an overview of the potential risks and redress measures in this context. For

example, in January 2019, ENISA issued its gap analysis into the security standards observed in the field of "Internet of Things."[30]

- ENISA has also strived to adopt guidance documents assisting companies in their day-to-day business practices, such as the adoption of good practices on the implementation of regulatory technical standards,[31] or the adoption of measures to reinforce trust and security in electronic communications and services.[32]

C. Reform of the ePrivacy Directive – the Draft EU ePrivacy Regulation Bill

As it was explained in the 2019 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.[33] In 2017, the draft ePrivacy Regulation was subject to an opinion of the WP29 (4 April 2017)[34] and an amended version was issued by the European Parliament (20 October 2017).[35]

Since then, internal discussions have been ongoing at the level of the Council of the EU during 2018 and 2019. Despite the progress made on this front, in November 2019, it was made public that the EU Council could still not find a common position on a variety of topics concerning the ePrivacy Regulation. Press reports have identified the following outstanding aspects as being at the origin of the disagreement among Member States:[36]

- The processing of electronic communications data for the purposes of prevention of child abuse imagery: Member States have diverging views on whether and how to achieve this objective.

- The protection of terminal equipment information: Member States have been reported to discuss extensively regarding conditional access to website content (so-called "cookie walls"), which underlies numerous existing business models. The positions of the Council and of the European Parliament differ vastly in this area.

- Processing of electronic communications data by third parties: While the latest draft proposal included a recital clarifying the concept of third parties, there are other ongoing discussions regarding whether the scope of these obligations should be extended to electronic communications providers in general, or to services covered by current sectoral legislation.

- Cooperation among data protection and telecommunications regulatory authorities: A number of Member States have raised concerns regarding the cooperation among various enforcement authorities.

In light of the disagreement among Member States within the Council, it has been reported that the European Commission has recently retrieved the ePrivacy Regulation bill, in order to update it in light of the various positions expressed by the Member States to date. The European Commission allegedly aims to resubmit a new ePrivacy Regulation bill for discussion during the Croatian Presidency of the Council (January to June 2020).[37]

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

As we indicated in the 2019 International Outlook and Review, the increasing impact of digital services in Europe and the overhaul brought about by the GDPR in the EU have led certain jurisdictions in the vicinity of the EU to improve and enforce more vigorously their data protection regulations.

A. Russia

Local data privacy laws have continued to be heavily enforced, reflecting the activity of the Russian Federal Service for the Supervision of Communications, Information Technology and Mass Communications ("**Roskomnadzor**") in monitoring and enforcing data protection compliance.

For example, in January 2019, it became public that the Roskomnadzor had sent letters to two social network services regarding their compliance with Russian data localization laws. In February and March 2019, the Roskomnadzor announced reports on administrative proceedings against these companies for alleged violations of Russian data protection laws.

In July 2019, Roskomnadzor imposed a 700,000 RUB fine (approx. 10,000 EUR) on Google for its alleged failure to remove prohibited search engine results. According to Roskomnadzor, more than a third of the links from a single Google search registry contained prohibited information under Russian law.

On 2 December 2019, the fines for violations of data localization and data processing requirements were increased. In particular, the failure by operators to collect, systemize and store personal data in Russian databases will be fined with 1 million to 6 million RUB (approx. 14,000 EUR to 84,500 EUR) for legal entities. In addition, the Law highlights that repeat offences will lead to fines up to 18 million RUB (approx. 250,000 EUR) for legal entities.

B. Switzerland

As indicated in the 2019 International Outlook and Review, to prepare for the entry into force of the GDPR, the Swiss government had issued a draft of a new Data Protection Act (the "**Draft FDPA**")[38] 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, in order to replace the Federal Act on Data Protection of 19 June 1992 (the "**FADP**").

In November 2019, the Swiss Federal Assembly announced that the State Political Commission of the Council of States ("**PCI-S**") had completed its detailed consultation on the Draft FDPA, which had been

unanimously accepted after consultation of the representatives of the cantonal data protection officers. In order to approach the Draft FDPA to the GDPR, the PCI-S departed from the decisions of the National Council, for example, including trade union membership as a category of sensitive personal data. It is therefore expected that the Draft FDPA will be adopted in the course of 2020.

C. Turkey

Throughout 2019, 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:

- Data protection obligations: On 18 March 2019, the KVKK issued guidelines on data protection in Turkey, addressing data processing requirements such as consent, transfers of data within and outside of Turkey, and data controller obligations, among other topics.

- Subject access requests: On 13 February 2019, the KVKK issued a decision on the time-frames to lodge a complaint with the KVKK further to a subject access request. The decision focuses on cases where a request made under the Turkish Data Protection Act was rejected, replied to insufficiently or not replied to in due time.

- Data processing registry: On 28 April 2019, the KVKK published a guide on the preparation of processing registry. The guide specifies the content of the registry and the preparation process, such as determining the purpose of the data processing and the data retention period.

- Data processing guide: On 6 August 2019, the KVKK published a guide, which aims at making it easier for companies to understand data protection requirements under the Turkish Data Protection Act, such as obligations of data disclosure, deletion, and anonymization, obligations to register with the data controller and exceptions to the obligation to handle a registry of operations, among other things.

- Transparency requirements: On 8 November 2019, the KVKK issued a statement on the transparency requirements, in order to bring the practices of companies in further compliance with the Turkish Data Protection Act. In January 2020, the KVKK announced the launch of its online portal on data violations, which is expected to increase the supervisory activity and enforcement actions of the KVKK.

Furthermore, the KVKK continued with its enforcement of the Turkish Data Protection Act. For example, in May 2019, the KVKK imposed fines up to 4.65 million TRY (approx. 250,000 EUR) on a social network service for its alleged failures to notify data breaches. In July 2019, the KVKK imposed a fine of 1.45 million TRY (approx. 220,000 EUR) on a hospitality company for an alleged data breach that affected Turkish citizens. Overall, the KVKK found and imposed fines over 1 million EUR on several companies for data breaches that occurred in several sectors.

III. Developments in Asia-Pacific and Africa

As we indicated in the 2019 International Outlook and Review, in an increasingly connected world, 2019 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 indicated in the 2019 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 they are exported.[39] 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.[40]

On 25 January 2019, the Ministry of Industry and Information Technology of the People's Republic of China ("**MIIT"**), the Cyberspace Administration of China ("**CAC**"), the Ministry of Public Security, and the State Administration for Market Regulation released a statement on privacy practices for applications. In particular, the announcement outlined the consent requirements from the perspective of the Chinese Cybersecurity Law, which requires controllers to provide privacy notices in clear, concise wording, to obtain freely given consent, to discourage "bundled" forms of consent, and to encourage app operators to provide an opt-out mechanism for personalized advertisements.

In March, the MIIT identified a number of organizations that had been involved in nuisance calls and the use of illegal apps to collect personal information. The MIIT noted that it had made arrangements for companies involved to immediately shut down phone lines used to facilitate the illegal calls. It also highlighted that it would cooperate with the Central Network Information Office, the Ministry of Public Security and the General Administration of Market Supervision in order to strengthen the protection of personal information collected by mobile apps.

The CAC has also been involved in the adoption of bills and rules regarding the protection of personal data in China, including the following:

- On 24 May 2019, the CAC published draft measures to enhance the security and management of critical information infrastructure, and launched a public consultation on the same topic.
- On 28 May 2019, the CAC published draft measures on data security management including, among others, provisions for privacy, data processing, notifications, and consent.
- On 31 May 2019, the CAC issued draft measures on the collection, storage, use, transfer and disclosure of children's personal information. The draft measures apply to children under 14 years of age and, among other things, specify that network operators should set up dedicated

children's personal information protection user agreements as well as designate personnel to be responsible for protecting children's personal information.

- On 13 June 2019, the CAC issued draft measures on cross-border data transfers. In particular, the draft measures require network operators to provide a declaration form, signed contract between network operators and receivers, and a security risk assessment, among other things, prior to personal information being transferred out of China.

- In July 2019, the CAC announced the release of an Internet information service complaint platform in order to facilitate and encourage data subjects to defend their rights.

B. Singapore

As indicated in the 2019 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 Commission gave businesses and organizations 12 months from the date of publication to review their processes and implement necessary changes to ensure compliance.[41]

Following the expiration of this grace period, the Singapore Personal Data Protection Commission ("**PDPC**") has initiated enforcement action and issued fines against numerous companies across all sectors for violations of Singapore data protection laws. For example, in January 2019, the PDPC imposed a fine of 750,000 SGD (approx. 500,000 EUR) on Integrated Health for data security failures.

C. India

As we indicated in the 2019 International Outlook and Review, the Indian 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**").[42]

In December 2019, after further deliberations, the Bill was approved by the Cabinet Ministry of India, and was tabled in the Indian Parliament by the Minister of Electronics and Information Technology. At the end of December 2019, the Bill started being analyzed by a Joint Parliamentary Committee in consultation with various groups.

D. Other Developments in Africa & Asia

Throughout 2019, a number of jurisdictions in Asia and Africa have adopted data protection legislation, including the following:

- Kenya: On 8 November 2019, the Kenya Data Protection Bill 2019 was signed into law.

- Nigeria: The National Information Technology Development Agency issued the Nigeria Data Protection Regulation 2019.

- Togo: In October 2019, Law No. 2019-014 Relating to the Protection of Personal Data was published in the Official Gazette.
- Uganda: In 2019, the Data Protection and Privacy Act entered into force.
- Indonesia: In October 2019, Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions became effective.
- New Zealand: In 2019, the Parliament discussed the Privacy Amendment Bill, which should become law in the course of 2020.
- Thailand: In May 2019, the Personal Data Protection Act and the Cybersecurity Act entered into force.

IV. Developments in Latin America and in the Caribbean Area

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

A. Brazil

As we indicated in the 2019 International Outlook and Review, a new General Data Protection Law was adopted in Brazil on 14 August 2018, after several years of discussions among decision-makers.[43]

In July 2019, the President of Brazil promulgated Law No 13.853 amending the General Data Protection Law. In its final form, the General Data Protection Law introduced some important revisions, such as the creation of an enforcement authority (the National Data Protection Authority), the extension of its application to public bodies as well as to private entities, the extensive appointment of Data Protection Officers, and the postponement of its application until 2022.

In the midst of the adoption of the General Data Protection Law, enforcement action of the Brazilian authorities has thrived to protect the privacy of its citizens. For example, on 30 December 2019, it was announced that the Ministry of Justice and Public Security had fined a social network service 6.6 million BRL (approx. 1.4 million EUR) for the alleged transfer to and misuse of personal data of Brazilian users by a political marketing consultancy firm.

B. Other Developments in the Caribbean Area

Throughout 2019, a number of jurisdictions in the Caribbean area have adopted data protection legislation, including the following:

- Barbados: In August 2019, the bill for the Data Protection Act 2019 was passed by the House of Assembly after its approval by the Senate.

- Cayman Islands: On 30 September 2019, the Data Protection Law, 2017 (Law 33 of 2017) entered into force.
- Jamaica: In July 2019, the Minister of Science, Energy and Technology had submitted to the Parliament a bill to reform the Data Protection Act 2017.

---

[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] The EDPB is an EU body that is formed by the representatives of the data protection authorities of the EU Member States, the EEA States (Iceland, Lichtenstein and Norway), and the European Data Protection Supervisor (the data protection agency that supervises the compliance of the EU institutions with EU data protection legislation). Under the GDPR, the EDPB has certain advisory, enforcement and decision-making powers.

[3] *See*: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.

[4] *See*: https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-opens-statutory-inquiry-twitter.

[5] *See*: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20191105-PM-Bussgeld_DW.pdf.

[6] *See*: here.

[7] *See*: here.

[8] *See*: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/.

[9] *See*: https://ico.org.uk/media/action-weve-taken/mpns/2616742/doorstop-mpn-20191217.pdf.

[10] *See*: https://edpb.europa.eu/news/national-news/2019/administrative-criminal-proceedings-austrian-data-protection-authority_en.

[11] *See*: https://edpb.europa.eu/news/national-news/2020/italian-supervisory-authority-fines-eni-gas-e-luce-eur-115-million-account_en.

[12] *See* CJEU, Case C-507/17 *Google LLC v. CNIL* (24 September 2019).

[13] *See* CJEU, Case C-673/17 *Verbraucherzentrale Bundesverband e.V. v. Planet49 GmbH* (1 October 2019).

[14] *See* CJEU, Case C-40/17 *Fashion ID GmbH & Co.KG v. Verbraucherzentrale NRW eV* (29 July 2019).

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

[16] *See* Opinion of Advocate General Saugmandsgaard Øe on Case C-311/18 *Data Protection Commissioner v. Facebook Ireland Limited*, *available here*.

[17] *See* Opinion of the Advocate General in the case C-311/18 *Facebook Ireland and Schrems*, *available here*.

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

[19] *See* General Court, Case T-738/16, *La Quadrature du Net and Others v. Commission*.

[20] *See* Report from the commission to the European parliament and the council on the third annual review of the functioning of the EU-U.S. Privacy Shield, *available here*.

[21] *See* "EU – U.S. Privacy Shield - Third Annual Joint Review," *available here*.

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

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

[24] *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/.

[25] *See* IAPP, "India to seek adequacy status with EU" (31 July 2019), *available at* https://iapp.org/news/a/india-to-seek-adequacy-status-with-eu/.

[26] *See* "Communication from the Commission to the European Parliament and the Council - Data protection rules as a trust-enabler in the EU and beyond – taking stock," *available here*.

[27] *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 here*.

[28] *See*: https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions, https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions-part-2, and https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices.

[29] *See*: https://www.enisa.europa.eu/publications/eu-ms-incident-response-development-status-report.

[30] *See*: https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis.

[31] *See*: https://www.enisa.europa.eu/publications/good-practices-on-the-implementation-of-regulatory-technical-standards.

[32] *See*: https://www.enisa.europa.eu/publications/reinforcing-trust-and-security-in-the-area-of-electronic-communications-and-online-services.

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

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

[35] *See*: here.

[36] *See*: https://iapp.org/news/a/how-the-eprivacy-regulation-failed-again/.

[37] *See*: https://www.euractiv.com/section/data-protection/news/commission-to-present-revamped-eprivacy-proposal/.

[38] 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 here.

[39] *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.

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

[41] *See* Singapore Personal Data Protection Commission, Proposed Advisory Guidelines on the Personal Data Protection Act For NRIC Numbers, published 7 November 2017, *available here*.

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

[43] *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/

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

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, the authors, or 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)20 7071 4250, jacox@gibsondunn.com)
Patrick Doris - London (+44 (0)20 7071 4276, pdoris@gibsondunn.com)
Bernard Grinspan - Paris (+33 (0)1 56 43 13 00, bgrinspan@gibsondunn.com)
Penny Madden - London (+44 (0)20 7071 4226, pmadden@gibsondunn.com)
Michael Walther - Munich (+49 89 189 33-180, mwalther@gibsondunn.com)
Kai Gesing - Munich (+49 89 189 33-180, kgesing@gibsondunn.com)
Alejandro Guerrero Perez - Brussels (+32 2 554 7218, aguerrero@gibsondunn.com)
Vera Lukic - Paris (+33 (0)1 56 43 13 00, vlukic@gibsondunn.com)
Sarah Wazen - London (+44 (0)20 7071 4203, swazen@gibsondunn.com)
Guillaume Buhagiar - Paris (+33 (0)1 56 43 13 00, gbuhagiar@gibsondunn.com)
Clémence Pugnet - Paris (+33 (0)1 56 43 13 00, cpugnet@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)
Debra Wong Yang - Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)
Matthew Benjamin - New York (+1 212-351-4079, mbenjamin@gibsondunn.com)
Ryan T. Bergsieker - Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)
Howard S. Hogan - Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com)
Joshua A. Jessen - Orange County/Palo Alto (+1 949-451-4114/+1 650-849-5375, jjessen@gibsondunn.com)
Kristin A. Linsley - San Francisco (+1 415-393-8395, klinsley@gibsondunn.com)
H. Mark Lyon - Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com)
Karl G. Nelson - Dallas (+1 214-698-3203, knelson@gibsondunn.com)
Deborah L. Stein (+1 213-229-7164, dstein@gibsondunn.com)
Eric D. Vandevelde - Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)
Benjamin B. Wagner - Palo Alto (+1 650-849-5395, bwagner@gibsondunn.com)

Michael Li-Ming Wong - San Francisco/Palo Alto (+1 415-393-8333/+1 650-849-5393, mwong@gibsondunn.com)