GIBSON DUNN

January 29, 2018

INTERNATIONAL CYBERSECURITY AND DATA PRIVACY OUTLOOK AND REVIEW – 2018

To Our Clients and Friends:

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

Like many recent years, 2017 saw significant developments in the evolution of the data protection and cybersecurity landscape outside the United States:

- Following the adoption of a General Data Protection Regulation governing the collection, processing and transfer of personal data in 2016 ("GDPR"),[1] several Member States of the European Union started to adapt their national legal frameworks in light of the future entry into application of the GDPR on 25 May 2018, and the Article 29 Working Party ("WP29") provided details regarding the implementation thereof.

- The first proposals for an upcoming European regulation with respect to private life and the protection of personal data in electronic communications, intended to repeal the currently applicable legal framework, were made public ("ePrivacy Regulation").

- The Member States of the European Union started working on the transposition into national law of the directive on the security of network and information systems ("NIS Directive").

- The framework for international data transfers between the U.S. and the European Union—the Privacy Shield—was subjected to various legal challenges.

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. Privacy Shield

On 12 July 2016, the European Commission formally approved the EU-U.S. Privacy Shield ("Privacy Shield"), a framework for navigating the transatlantic transfer of data from the EU to the United States. The Privacy Shield replaces the EU-U.S. Safe Harbor framework, which was invalidated by the European Court of Justice ("ECJ") on 6 October 2015 in *Maximilian Schrems v. Data Protection Commissioner* (the "*Schrems*" decision).[2] We provided an in-depth discussion of the *Schrems* decision in a previous Outlook and Review.[3]

1. Reviews of the European Commission and the WP29

Following the adoption of the Privacy Shield, the WP29—an advisory body that includes representatives from the data protection authorities of each EU Member State—stated that "the national representatives of the WP29 will not only assess if the remaining issues have been solved but also if the safeguards provided under the EU-U.S. Privacy Shield are workable and effective" during a joint annual review of the Privacy Shield mechanism.[4]

The first review was conducted in mid-September 2017 by the European Commission and U.S. authorities. The European Commission published its report on 18 October 2017.[5] It concluded that the Privacy Shield continues to ensure an adequate level of protection, noting that various important structures and procedures have been put in place by U.S. authorities—namely, new redress possibilities for EU nationals, a complaint-handling and enforcement procedure, an increased level of cooperation with EU data protection authorities, and necessary safeguards for government access to personal data. Overall, the European Commission determined that the framework, including the self-certification process, is functioning well, and the European Commission continues to support the Privacy Shield. The European Commission did, however, make several recommendations to further improve the Privacy Shield's functioning:

- More proactive and regular monitoring of companies' compliance with their obligations under the Privacy Shield by the U.S. Department of Commerce, including the use of review questionnaires or annual compliance reports.
- Increased searches for and enforcement against companies that falsely claim to participate in the Privacy Shield by U.S. authorities.
- Raising awareness of how EU individuals can exercise their rights under the Privacy Shield, particularly how they can submit complaints.
- Closer cooperation between EU and U.S. authorities to achieve a consistent interpretation and to develop guidance for companies and enforcers.
- The appointment of a permanent Privacy Shield Ombudsman and the appointment of additional members to the Privacy and Civil Liberties Oversight Board ("PCLOB").
- A codification of Presidential Policy Directive 28 ("PPD-28"), as part of the reauthorization and reform of Section 702 of the Foreign Intelligence Surveillance Act ("FISA").

It should be noted on this last point that on 19 January 2018 the United States renewed FISA Section 702 without enshrining the protections set forth in the PPD-28.[6] It remains to be seen how this, and the success of efforts to follow up on the other recommendations, will affect the next annual review of the Privacy Shield in fall 2018.

On 28 November 2017, the WP29 released its own opinion on the first annual joint review of the Privacy Shield mechanism.[7] The WP29's findings are quite different from the Commission's, as the WP29

identified "significant concerns" with the Privacy Shield's mechanisms as currently operated. While the WP29 recognized the Privacy Shield as an improvement compared to the invalidated Safe Harbor mechanism, and welcomed the increased transparency of the U.S. government and legislator regarding the use of their surveillance powers, the WP29 set forth several recommendations, namely:

- U.S. authorities should provide more guidance on the principles of the Privacy Shield, particularly regarding transfers, available rights, and recourses and remedies, to make it easier for companies to interpret their obligations and individuals to exercise their rights.
- More oversight by U.S. authorities concerning compliance with Privacy Shield principles—for instance, compliance with limits on monitoring—and more proactive supervision of the participating organizations.
- Distinguishing the status of processors and controllers established in the U.S., as the opinion notes there is currently no differentiation made during the application process between the two.
- Increasing the level of protection concerning profiling data or automated decision-making by creating specific rules to provide sufficient safeguards.
- Avoiding exceptions for the processing of Human Resources ("HR") data, as according to the WP29 the U.S. Department of Commerce considers HR data too narrowly, allowing for the transfer of some HR data as commercial data.
- Shoring up safeguards against the access of data by U.S. public authorities.
- Addressing the lack of a permanent and independent Ombudsman and the several vacancies on the PCLOB.

The WP29 warned that should their concerns fail to be addressed, the group would then take appropriate actions, including challenging the Privacy Shield before national courts. The WP29 therefore called on the European Commission and U.S. authorities to resume discussions, and to set up an action plan to demonstrate that these concerns will be addressed.

2. Challenges to Privacy Shield

Advocacy groups have already filed challenges to the Privacy Shield. Specifically, in October 2016 Digital Rights Ireland ("DRI") filed a challenge with a Luxembourg-based General Court, a lower court of the ECJ, to annul the European Commission's 12 July 2016 Adequacy Decision, which approved and adopted the Privacy Shield.[8] However, this action was dismissed by the General Court of the European Union on 22 November 2017.[9] The European judges held that DRI neither had an interest in bringing proceedings in its own name nor had standing to act in the name of its members and supporters or on behalf of the general public. This is not the only challenge to the Privacy Shield, however: In 2016, a French privacy advocacy group also challenged the Adequacy Decision in a legal action to the ECJ, claiming that the U.S. Ombudsman redress mechanism is not sufficiently independent and effective and therefore the Adequacy Decision must be annulled.[10] This case remains ongoing.[11]

B. EU Data Protection Regulation and Reform

1. GDPR

On 15 December 2015, the European Commission, the European Parliament, and the European Council agreed to an EU data protection reform to boost the EU Digital Single Market. The bill was adopted by the European Council and the European Parliament in early April 2016 and came into force on 24 May 2016 as the GDPR. However, the GDPR provides for a two-year "grace period," such that it will not become fully applicable until 25 May 2018. The GDPR replaces the EU Data Protection Directive[12] and constitutes a set of data protection rules that are directly applicable to the processing of personal data across EU Member States (for additional details regarding the main requirements of the GDPR, please refer to Section 2 below).

2. Principal Elements of the GDPR

The core substantive elements of the GDPR, which will become fully applicable in May 2018, include the following:

- **Extraterritorial Scope**: The GDPR will cover not only data controllers established in the EU, but will also apply to organizations that offer goods or services to residents in the EU, even if these organizations are not established in the EU and do not process data using servers in the EU.[13]

- **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 late 2017, the WP29 made draft Guidelines on transparency public.[14] Even though the final version of this document is not available yet, the purpose of such Guidelines is to provide practical guidance and interpretative assistance on the new transparency obligations as resulting from the GDPR.

- **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 November 2017, the WP29 adopted Guidelines specifically dedicated to the concept of consent and focusing on the changes in this respect resulting from the GDPR.[15]

- **"Right to Be Forgotten"**: The GDPR further develops the "right to be forgotten" (formally called 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.[16] This right was already introduced in the EU Data Protection Directive, and was the object of the litigation before the CJEU in *Google Spain SL and Google Inc. v. AEPD and Mario Costeja González*.[17]

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 Data Protection Authority/ies ("DPA(s)") without undue delay and, in any event, within 72 hours after having become 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.[18]

- **Profiling Activities**: The GDPR specifically addresses the use of profiling and other automated individual decision-making. In 2017, the WP29 made Guidelines public in this respect.[19] These clarify the provisions of the GDPR regarding profiling, in particular by defining in more detail what profiling is.

- **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.[20] However, the GDPR does not specifically detail the criteria to be taken into account for determining whether given processing activities represent "high risk." Instead, the GDPR provides a non-exhaustive list of examples falling within this scope. Similarly, no process for performing DPIAs is detailed as part of the GDPR. Considering the need for additional information in this respect, the WP29 issued Guidelines in 2017 intended to clarify which processing operations must be subject to DPIAs and how they should be carried out.[21] These Guidelines were subsequently revised throughout the year.[22]

- **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 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. The WP29 has also called industry stakeholders and trade associations to work together on a common set of interoperable standards and formats to deliver the requirements of the right to data portability.[23] In 2017, the WP29 issued revised 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.[24]

- **Competent Supervisory Authority**: To date, in the EU the monitoring of the application of data protection rules has fallen almost exclusively under the jurisdiction of national DPAs. Subject to the EU Data Protection Directive and the case law of the CJEU, DPAs only had jurisdiction to find a violation of their data protection laws and impose fines where, *inter alia*, their respective national laws were applicable.[25]

  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.[26]

  - *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.[27] 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 European Data Protection Board ("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.[28]

  - *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.[29]

  - In 2016, the WP29 issued Guidelines that aim to assist controllers and processors in the identification of their lead DPA.[30] These Guidelines were updated in 2017, in particular for addressing circumstances involving joint data controllers.[31]

- **Governance**: Data controllers and processors may be required to designate a Data Protection Officer ("DPO") in certain circumstances. Small and medium-sized enterprises will be exempt from the obligation to appoint a data protection officer insofar as data processing is not their core

business activity. The WP29 has issued Guidelines that clarify the conditions for the designation, position and tasks of the DPO to ensure compliance with the GDPR; these Guidelines were revised in 2017.[32]

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 4% of their global annual turnover.

3. National Data Protection Reforms Implementing the GDPR

Because the GDPR is a regulation, there is no need for Member States of the European Union 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. Another example is to be found under Article 58 of the GDPR, as Member States may provide by law that their supervisory authorities have additional powers beyond those already specified under the GDPR.

Below is an overview of the national data protection reforms implemented throughout the European Union during 2017:

Member State	Status of National Data Protection Reform
Austria	The Datenschutz-Anpassungsgesetz 2018 was published in July 2017. This act is expected to support the application of the GDPR and will enter into effect by 25 May 2018. The Datenschutzgesezt 2000 will be replaced accordingly.
Belgium	Belgium is currently adapting its national data protection legal framework by: · reforming the Belgian Privacy Commission (the draft bill in this respect was adopted by the Parliament on 16 November 2017 and was submitted for the King's approval); and · preparing a framework law for addressing the national considerations resulting from the GDPR (although no draft has been disclosed yet).

Member State	Status of National Data Protection Reform
Bulgaria	In 2017, Bulgaria did not enact or propose a bill concerning GDPR-related privacy issues.
Croatia	In 2017, Croatia did not enact or propose a bill concerning GDPR-related privacy issues.
Cyprus	In 2017, Cyprus did not enact or propose a bill concerning GDPR-related privacy issues.
Czech Republic	A draft Data Protection Act, intended to adapt the current national legal framework to the GDPR, was discussed by the government. The upcoming Data Protection Act is expected to replace the current act on data protection.
Denmark	On 25 October 2017, a proposal for a new Data Protection Act implementing the GDPR was made public. This proposal was discussed by the Danish Parliament in late 2017 and is expected to pass in the first months of 2018.
Estonia	The Ministry of Justice rendered public a first draft of the legislation intended to implement the GDPR. However, the draft was not submitted to Parliament for review in 2017.
Finland	A working group set up by the Ministry of Justice issued a report in June 2017 proposing to replace the current Finnish Data Protection Act with a new act intended to supplement the GDPR when the GDPR enters into application.
France	A draft data law intended to modify the current French Data Protection Act was made public in December 2017. It is likely that this initial draft will go through subsequent modifications before the final law is eventually passed.
Germany	In June 2017, Germany adapted its Data Protection Act to the GDPR. The previous version of the German Data Protection Act will remain in force until 25 May 2018.

Member State	Status of National Data Protection Reform
Greece	In 2017, Greece did not enact or propose a bill concerning GDPR-related privacy issues.
Hungary	In 2017, Hungary launched a public consultation on a proposal to amend the current Hungarian Data Protection Act. This proposal is expected to become final in early 2018.
Ireland	In May 2017, Ireland issued a General Scheme of Data Protection Bill providing a general scheme for the act intended to give effect to and complement the GDPR.
Italy	On 6 November 2017, the Italian Parliament passed a law (Law No. 163) adopting specific provisions with respect to the GDPR. The currently applicable Italian Data Protection Code is to be modified within 6 months from the passage of Law No. 163.
Latvia	Latvia made public a draft Personal Data Processing Law in October 2017.
Lithuania	The law applicable in Lithuania (i.e., the Lithuanian Law on Legal Protection of Personal Data) is currently being amended so as to integrate the requirements of the GDPR.
Luxembourg	The government of Luxembourg proposed a bill specifically addressing data protection in order to adapt the local law to the requirements of the GDPR.
Malta	In 2017, Malta did not enact or propose a bill concerning GDPR-related privacy issues.
Netherlands	The data protection law currently applicable in the Netherlands results from the Dutch Personal Data Protection Act (*Wet bescherming persoonsgegevens*). This Act will no longer be applicable after the GDPR enters into effect in May 2018.

Member State	Status of National Data Protection Reform
Poland	In September 2017, Poland published a draft Personal Data Protection Act, intended to provide a legal framework for the GDPR. This draft was made subject to public consultations and is expected to be enacted in 2018, prior to the entry into application of the GDPR.
Portugal	In 2017, Portugal did not enact or propose a bill concerning GDPR-related privacy issues.
Romania	Draft legislation for implementing the GDPR was disclosed and submitted for public debate in 2017.
Slovakia	On 29 November 2017, the Slovakian Data Protection Act was adopted by the Slovak Parliament with an entry into force on the same date as the GDPR.
Slovenia	The currently applicable Slovenian Data Protection Act is expected to be repealed by a new data protection act ("ZVOP-2") intended to ensure the proper implementation of data protection requirements following the entry into application of the GDPR. ZVOP-2 was subject to the legislative process in 2017 and is likely to be adopted in early 2018.
Spain	A bill regarding data protection intended to amend the current legal framework was published and made subject to debate, with an eye toward eventual approval by the Spanish Parliament.
Sweden	A report of the Swedish government proposing provisions intended to complement the GDPR was issued in May 2017, but no government bill was passed in this respect during 2017.

Member State	Status of National Data Protection Reform
United Kingdom	On 14 September 2017, the Data Protection Bill was published with the aim to modernize data protection law. Even though the Data Protection Bill has a wider scope than the mere adaptation of national law to the GDPR, one of its core features includes detailing how the UK uses the flexibility granted by the GDPR to Member States with respect to specific data protection issues.

C. EU Cyber Security Directive

On 6 July 2016, the European Parliament officially adopted the Network and Information Security ("NIS") Directive[33] which is expected to be fully applicable (via national regulations) as of May 2018. The NIS Directive is the first set of cybersecurity rules to be adopted on the EU level, adding to an already complex array of laws with which companies must comply when implementing security and breach response plans. 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.

In February 2017, the European Agency for Network and Information Security ("ENISA") issued guidelines related to incident notification for digital service providers in the context of the NIS Directive, in order to provide practical information on the cases covered by the NIS Directive and the actions to be taken in such a case.[34]

More details as to how the NIS Directive will be implemented at local level were also disclosed in 2017 as Member States started to adopt national legislation to transpose the NIS Directive. For example, in France on 19 December 2017, a national bill for transposing the NIS Directive was adopted by the French Senate. This bill specifies fines up to EUR 100,000 if officers of essential services providers do not comply with the security requirements specified by the French Prime Minister and fines up to EUR 75,000 if such officers do not comply with the obligation to provide notifications of data breaches. Regarding legal persons, the fines for non-compliance with the security requirements specified by the French Prime Minister can be up to EUR 500,000, and up to EUR 375,000 in case data breaches are not duly notified.

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

- Essential service providers include actors in the energy, transport, banking and financial markets, as well as health, water and digital infrastructure[35] 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.

In terms of geographic scope, the NIS Directive aims to address potential incidents taking place "*within the [European] Union*"[36] and will apply to all entities providing the above services[37] within the EU territory/to EU residents, regardless of their physical location. In particular, all digital service providers that are not established in the EU, but offer services covered by the NIS Directive within the EU, are required to designate an EU-based representative.[38]

Companies covered by the NIS Directive will have to ensure that their digital infrastructure is robust enough to withstand cyber-attacks and may need to report major security incidents to the national authorities. Businesses will also be required to apply procedures demonstrating effective use of security policies and measures.

1. Digital Service Providers

Digital service providers will be obliged to report all incidents that have a "substantial impact" on their services (in terms of the duration, geographic spread and the number of users affected by the incident).[39] It will be up to regulators to decide whether to inform the public about these incidents after consulting the company involved.

As a practical matter, the NIS Directive states that jurisdiction over a digital service provider should be attributed to the Member State in which it has its main EU establishment, which in principle corresponds to the place where the provider has its head office in the EU.[40] Digital service providers not established in the EU will be deemed to be under the primary jurisdiction of the Member State where their EU representative has been appointed.[41]

Notably, where an incident involves personal data, there may be an additional requirement to report to DPAs under the GDPR, which will come into effect on 25 May 2018. As indicated above, the GDPR will also have a reporting provision for data breaches, although the notification obligation will focus on the protection of personal information, in contrast to the NIS Directive's data reporting requirement which is aimed at improving computer and information technology systems overall. Thus, it is possible that a single cybersecurity breach will need to be notified to more than one authority in each EU Member State affected.

2. Member State Obligations

The NIS Directive itself is not directly applicable. It will first have to be transposed and implemented into national law by the Member States by May 2018. Member States will need to, for example, designate the competent national authorities, identify operators of essential services, indicate which types of incidents they must report and establish sanctions for failure to notify.[42] National procedural rules (for both administrative and court proceedings) will govern the application of the NIS Directive and the relevant national laws to affected entities.[43]

In addition, each Member State is to adopt a national strategy to maintain the security of network and information systems and will designate one or more national competent authorities to monitor the application of the NIS Directive. They are also to designate one or more Computer Security Incident

Response Teams ("CSIRTs") responsible for monitoring and responding to incidents and providing early warnings about risks.

3. Minimum Harmonization and Coordination Among EU Member States

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, the NIS Directive gives 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.[44] Thus, despite the ability of Member States to seek the assistance of the 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).[45]

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 on such entities.[46] The European Commission retains powers to adopt implementing rules regarding the application of the security and notification requirements rules applicable to digital service providers.[47] It is expected that these rules will be developed in cooperation with the ENISA and stakeholders, and will enable uniform treatment of digital service providers across the EU. In addition, the competent authorities will be able to exercise supervisory activities only when provided with 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.

D. Other EU Developments

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

2016 has seen 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, a draft of the future EU ePrivacy Regulation (the "draft ePrivacy Regulation") was leaked in December 2016.[48] Such draft was followed by the release of the European Commission's final proposal on 10 January 2017,[49] which, despite some changes, is mostly similar to the leaked version. Later in 2017, the European Commission's proposal was followed by an Opinion of the WP29 released on 4 April 2017.[50] The European Parliament also proposed an amended version thereof on

20 October 2017,[51] and discussions at the Council of the European Union are still ongoing to date to adopt a final proposal, even though a first redraft has already been published.[52]

a. The European Commission's ePrivacy Regulation proposal

The Commission's ePrivacy Regulation proposal released in January 2017 seeks 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 constitutes 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 draft instrument that is deemed to replace the ePrivacy Directive is a Regulation. Under EU law, a Directive is an instrument that only binds EU Member States as to its content and objectives; it cannot be directly applied against individuals, and needs to be transposed into national laws and regulations for its terms to be fully effective. The ePrivacy Directive has been incorporated into numerous different acts and regulations at national level, which are subject to uneven enforcement by the respective national authorities.

  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. 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 demonstrate alignment with the GDPR. For example, as with the GDPR, the draft ePrivacy Regulation has a broad territorial scope and applies 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 aims 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. The regime for sanctions is also aligned with the GDPR, foreseeing the possibility that organizations be imposed fines up to EUR 20 million or 4% of their worldwide annual turnover for certain infringements (e.g., breaches of secrecy requirements, cookies requirements and the rules on the use of metadata).

  From a substantive perspective, the definition of a number of legal concepts used in both the GDPR and in the draft ePrivacy Regulation has also been 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] This expansion in scope is achieved by the broad definition of "electronic communications services" of the draft, and is consistent with the current regulatory overhaul that is ongoing in the field of electronic communications.[54]

- **Cookies and Other Connection Data**: Like the ePrivacy Directive, the draft ePrivacy Regulation contains a provision that addresses the circumstances under which the storage and collection of data on users' devices is lawful. These practices can continue to be based on the prior consent obtained from users. Absent users' consent, according to the draft ePrivacy Regulation, it will still be possible to carry out these practices provided that:[55]

    - 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 suggest that the circumstances in which consent is not required can be interpreted more broadly than under the current ePrivacy Directive.[56] For example, first-party analytics cookies, cookies used to give effect to users' website preferences and cookies required to fill out online forms could be understood to be exempt from the consent requirement.[57]

  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." Under the current draft, this collection may only occur "if it is done exclusively in order to, for the time necessary for, and for the purpose of establishing a connection," and is subject to significant information and consent requirements.[58] **Marketing Communications**: The draft ePrivacy Regulation requires all end users (including corporate and individual subscribers) to consent to direct marketing communications undertaken via electronic communications services. While telephone marketing continues to be permitted on an opt-out basis, the draft ePrivacy Regulation requires entities placing marketing calls to use a specific code or prefix identifying it as a marketing call.[59]

- **Supervisory Authorities and EDPB**: One of the novelties introduced by the draft ePrivacy Regulation is a section devoted to the appointment and powers of national supervisory authorities.[60] 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. Finally, the EDPB is empowered to ensure the consistent application of the relevant provisions of the draft ePrivacy Regulation.

- **Implementation**: The draft provides for the ePrivacy Regulation to enter into force on 25 May 2018, at the same time as the GDPR. However, it is highly unlikely to come into force on that date, or even any time later in 2018.

b. The WP29 Opinion on the European Commission Proposal

Following the release of the European Commission's proposal, the WP29 released its opinion on the proposed regulation in April 2017[61]. The WP29 stated that it "welcomes the proposal" and "the choice for a regulation as the regulatory instrument." More broadly, it supported the approach of the regulation and its broad scope, along with its principle of "broad prohibitions and narrow exceptions." However, 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. It is interesting to note that this was initially in the Commission's leaked draft but not in its final proposal.

The WP29 expects that their concerns will 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 proposal.[62] It draws on some of the propositions made by the WP29. For example, the Parliament's version is more stringent on the use of personal data, and 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.

In addition to the Parliament's version, the Council of the European Union has also published a working proposal.[63] However it is merely a draft of the presidency of the Council, which has yet to adopt a final proposal. Bulgaria, which takes the presidency of the Council of the European Union during the first half of 2018 has indicated it intends to focus on moving negotiations ahead on the ePrivacy Regulation.[64] Tripartite negotiations will then need to begin in order to agree upon a common text to be adopted. In any case, it most likely will not be adopted by May 2018 as initially planned.

2. CJEU Case Law

2017 has also witnessed important cases before the Court of Justice of the European Union ("CJEU").

a. The Determination of the Data Controller and Applicable Law

Under the EU Data Protection Directive, the applicability of the data protection laws of a Member State depends primarily on the existence of a relevant "establishment" in that Member State. In the past years, the concept of "establishment" gave rise to considerable debate. (See, for example, the 2016 ruling in the *Verein für Konsumenteninformation v. Amazon EU Sàrl* case[65], repeating the CJEU's findings in the *Weltimmo* judgment of 1 October 2015[66] where it defined broadly the concept of "establishment" contained in Article 4(1)(a) of the EU Data Protection Directive.) While the CJEU has indicated that the absence of "a branch or subsidiary in a Member State does not preclude [the controller] from having an establishment there within the meaning of Article 4(1)(a)" (e.g., through the existence of other stable arrangements, like an office), such an establishment cannot be presumed to exist "merely […] because the undertaking's website is accessible there."

Regarding the interpretation of the notion of "establishment,", additional information was brought to light in the course of 2017. Indeed, on 24 October 2017 Advocate General Bot made his opinion public regarding the determination of the applicable law in a case where data processing activities were performed through a social media page.[67] A German company set up a fan page through a U.S.-based social network, which provided statistics based on the personal data of the visitors (such as their preferences and habits) to the company administrating the fan page. The data protection authority of Schleswig-Holstein required the German company to shut down its fan page as neither the social media site nor the company itself allegedly informed visitors that their personal data was used for this particular purpose.

The German Federal Administrative Court sought a preliminary ruling from the CJEU, requesting clarification. In his opinion, Advocate General Bot first determined that the company administrating the fan page was a joint controller with the social media company regarding the collection of personal data.

Second, Advocate General Bot held that data processing is carried out in the context of the activities of an establishment of the controller on the territory of a Member State when an undertaking, operating a social network, sets up in that Member State a subsidiary which is intended to promote and sell advertising space offered by that undertaking and which directs its activities toward residents in that Member State.[68] It is worth noting yet that the opinion of Advocate General Bot in this respect is controversial.

A ruling from the CJEU, which could either follow the opinion of Advocate General Bot or depart therefrom, is expected in 2018.

b. Claims Assignment

On 14 November 2017, Advocate General Bobek delivered his opinion on the *Maximilian Schrems v. Facebook Ireland Limited* case pending in the CJEU.[69]

Mr. Schrems had 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. 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.

c. Outlook

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.[70] If the CJEU were to decide to invalidate the standard contractual clauses, this ruling would in all likelihood have tremendous impact on businesses around the world, many of which rely on these legal warranties to ensure an adequate level of data protection to data transfers outside the European Union.

3. Article 29 Working Party (WP29) Opinions

As indicated above, during 2017 the WP29 issued several Guidelines concerning the application of the GDPR to the right to data portability, the appointment and duties of DPOs, the identification of lead DPAs, the concepts of consent and transparency, and other issues. In parallel, within the framework of the GDPR, the WP29 also adopted Guidelines intended for use by the supervisory authorities to ensure better application and enforcement of the GDPR regarding the application and setting of administrative fines.[71]

In addition to the abovementioned Guidelines, the WP29 issued various opinions regarding the key issues of the Law Enforcement Directive No. 2016/680,[72] data processing in the context of Cooperative Intelligent Transport Systems (C-ITS),[73] and data processing at work,[74] as well as the draft ePrivacy Regulation proposal.[75]

The WP29 also rendered public some working documents on the adequacy referential within the framework of data transfers to third countries[76] and the elements and principles to be found in Binding Corporate Rules.[77]

II. Asia-Pacific and Other Notable International Developments

In an increasingly connected world, 2017 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:

- On 1 June 2017, China's Cybersecurity Law went into effect, becoming the first comprehensive Chinese law to regulate how companies manage and protect digital information. 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.[78]

  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.[79] 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.[80] 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.[81] 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.[82] 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.

- With the growing threat of hacking and identity theft, the Personal Data Protection Commission of Singapore issued proposed advisory guidelines on 7 November 2017 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 is giving businesses and organizations 12 months from publication to review their processes and implement necessary changes to ensure compliance.[83]

- Several other countries, such as Australia and Turkey, also sought to address privacy issues and published important guidelines regarding procedures for deleting, destroying, and anonymizing personal data. Other countries like Argentina forged ahead with an overhaul of the country's data protection regime by publishing a draft data protection bill that would align the country's privacy laws with the GDPR requirements of the European Union.[84]

- There has also been civic engagement with the public as a number of countries solicited public comments to certain proposed regulations. For example, Canada opened up for comments a proposed regulation that would mandate reporting of privacy breaches under its Personal Information Protection and Electronic Documents Act of 2015, while India recently issued a white paper inviting comments that would inform the legal framework for drafting a data protection bill to "ensure growth of the digital economy while keeping personal data of citizens secure and protected."[85]

---

[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 (General Data Protection Regulation), OJ L 119, 4.5.2016, pp. 1-88, *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

[2] Case C-362/14, *Maximillian Schrems v. Data Protection Commissioner* (Oct. 6, 2016), European Court of Justice.

[3] For a detailed analysis of the *Schrems* decision, please see Gibson Dunn Client Alert: Cybersecurity and Data Privacy Outlook and Review: 2016 (Jan. 28, 2016) *available at* http://www.gibsondunn.com/publications/Pages/Cybersecurity-and-Data-Privacy-Outlook-and-Review--2016.aspx.

[4] http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf.

[5] http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605619.

[6] https://www.whitehouse.gov/briefings-statements/statement-president-fisa-amendments-reauthorization-act-2017/.

[7] http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48782.

[8] http://curia.europa.eu/juris/document/document.jsf?text=&docid=185146&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=320298

[9] Order of the General Court of the European Union, Digital Rights Ireland v. Commission, 22 November 2017, T-670/16.

[10] http://curia.europa.eu.

[11] http://curia.europa.eu.

[12] *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.

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

[14] *See* WP29, *Guidelines on Transparency under Regulation 2016/679* (WP260; draft not adopted yet), *available at* http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

[15] *See* WP29, *Guidelines on Consent under Regulation 2016/679* (WP259; 28 November 2017), *available at* http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

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

[17] *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.

[18] *See* WP29, *Guidelines on Personal Data Breach Notification under Regulation 2016/679* (WP250; 3 October 2017), *available at* http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

[19] *See* WP29, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (WP251; 3 October 2017).

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

[21] *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; 4 April 2017), *available at* http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

[22] *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; 4 October 2017), *available at* http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

[23] *See* WP29, *Guidelines on the right to data portability* (WP 242; 13 December 2016), *available at* http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf.

[24] *See* WP29, *Guidelines on the right to data portability* (WP242 rev.01; 5 April 2017), *available at* http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

[25] *See* EU Data Protection Directive, at Articles 4(1) and 28; and Case C-230/14 *Weltimmo s.r.o v. Nemzeti Adatvédelmi és Információszabadság Hatóság* ECLI:EU:C:2015:639.

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

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

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

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

[30] *See* WP29, *Guidelines for Identifying a Controller or Processor's Lead Supervisory Authority* (WP 244; 13 December 2016), *available at* http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_en_40857.pdf.

[31] *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.

[32] *See* WP29, *Guidelines on Data Protection Officers ('DPOs')* (WP243 rev.01; 5 April 2017), *available at* http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

[33] *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.

[34] *See* ENISA, *Incident Notification for DSPs in the Context of the NIS Directive: A Comprehensive Guideline on How to Implement Incident Notification for Digital Service Providers, in the Context of the NIS Directive*, February 2017, *available at* https://www.enisa.europa.eu/publications/incident-notification-for-dsps-in-the-context-of-the-nis-directive/.

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

[36] *See* NIS Directive, at Article 1(1).

[37] With regard to essential services, the NIS Directive will apply to all entities identified by the respective national authorities as "*essential*" providers of such services in that Member State, see NIS Directive, at Article 5(2).

[38] *See* NIS Directive, at Article 18(2).

[39] *See* NIS Directive, at Article 16(3).

[40] *See* NIS Directive, at Article 18(1). This criterion will not depend on whether the network and information systems are physically located in a given place. *See* NIS Directive, at Recital 64.

[41] *See* NIS Directive, at Article 18(2).

[42] Member States will have an additional six months *after* the transposition into national law to identify operators of essential services (i.e., a total of 27 months). *See* NIS Directive, at Article 5(1).

[43] These should respect the fundamental rights of the effective remedy and the right to be heard. *See* NIS Directive, at Recital 75.

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

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

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

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

[48] *See* Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and personal data in electronic communications and repealing Directive 2002/58/EC ('Privacy and Electronic Communications Regulation'), *available at* http://www.politico.eu/wp-content/uploads/2016/12/POLITICO-e-privacy-directive-review-draft-december.pdf.

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

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

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

[52] https://iapp.org/resources/article/council-of-the-eu-eprivacy-regulation-proposal-december-2017/.

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

[54] *See*, e.g., Proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code (Recast), COM/2016/0590, *available at* http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=comnat:COM_2016_0590_FIN.

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

[56] 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.

[57] *See* draft ePrivacy Regulation, at Recital (25).

[58] *See* draft ePrivacy Regulation, at Article 8(2).

[59] *See* draft ePrivacy Regulation, at Article 16.

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

[61] *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.

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

[63] *See* Council of the European Union's working proposal *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_11995_2017_INIT&from=EN.

[64] https://www.euractiv.com/section/digital/news/bulgaria-makes-telecoms-overhaul-a-focus-during-council-presidency/.

[65] *See* Case C-191/15 *Verein für Konsumenteninformation v. Amazon EU Sàrl available at http://curia.europa.eu/juris/document/document.jsf?text=&docid=182286&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1126849*.

[66] *See* Case C-230/14 *Weltimmo s.r.o v. Nemzeti Adatvédelmi és Információszabadság Hatóság* ECLI:EU:C:2015:639.

[67] *See*, Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH*.

[68] *See* Opinion of Advocate General Bot delivered on 24 October 2017, Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH*.

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

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

[71] *See* WP29, *Guidelines on the Application and Setting of Administrative Fines for the Purposes of the Regulation 2016/679* (WP253; 3 October 2017), *available at* http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

[72] *See* WP29, *Opinion on Some Key Issues of the Law Enforcement Directive (EU 2016/680)* (WP258; 29 November 2017), *available at* http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

[73] *See* WP29, *Opinion 03/2017 on Processing Personal Data in the Context of Cooperative Intelligent Transport Systems (C-ITS)* (WP252; 4 October 2017), *available at* http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

[74] *See* WP29, *Opinion 2/2017 on Data Processing at Work* (WP249; 8 June 2017), *available at* http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

[75] *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.

[76] *See* WP29, *Adequacy Referential (updated)* (WP254; 28 November 2017), *available at* http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

[77] *See* WP29, *Working Document Setting up a Table with the Elements and Principles to be Found in Binding Corporate Rules* (WP256 and WP257; 29 November 2017), *available at* http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

[78] *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.

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

[80] 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.

[81] 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.

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

[83] 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.

[84] Office of the Australian Information Commissioner, "De-identification Decision-Making Framework", Australian Government (Sept. 18, 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* (Sept. 26, 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 (Sept. 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.

[85] Naïm Alexandre Antaki and Wendy J. Wagner, "No escaping notification: Government releases proposed regulations for federal data breach reporting & notification", *Lexology* (Sept. 6, 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 (Nov. 27, 2017), *available at* http://meity.gov.in/white-paper-data-protection-framework-india-public-comments-invited.

The following Gibson Dunn lawyers assisted in the preparation of this client alert: Ahmed Baladi, Alexander Southwell, Ryan Bergsieker and Bastien Husson.

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 - 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)
Bernard Grinspan - Paris (+33 (0)1 56 43 13 00, bgrinspan@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)
Nicolas Autet - Paris (+33 (0)1 56 43 13 00, nautet@gibsondunn.com)
Kai Gesing - Munich (+49 89 189 33-180, kgesing@gibsondunn.com)
Sarah Wazen - London (+44 (0)20 7071 4203, swazen@gibsondunn.com)
Emmanuelle Bartoli - Paris (+33 (0)1 56 43 13 57, ebartoli@gibsondunn.com)
Alejandro Guerrero Perez - Brussels (+32 2 554 7218, aguerreroperez@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 - Chair, PCCP Practice, New York (+1 212-351-3981, asouthwell@gibsondunn.com)
Caroline Krass - Chair, National Security Practice, Washington, D.C. (+1 202-887-3784, ckrass@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)
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)
Ryan T. Bergsieker - Denver (+1 303-298-5774, rbergsieker@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 Disclosure 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)