National Legal Data Protection Regimes

A Comparative Analysis of Six Countries

January 2020

UNITED NATIONS FOUNDATION | BILL & MELINDA GATES foundation | SWEDEN | USAID FROM THE AMERICAN PEOPLE

Contents

Acknowledgements 2

Disclaimer 2

Background 3

Introduction 5

What are global legal standards for processing personal data? 6

- European Union 6
- China 9
- United States 10
- India 13
- Colombia 16
- United Arab Emirates 18

What are global legal standards for securing personal data? 21

- European Union 21
- China 21
- United States 22
- India 22
- Colombia 23
- United Arab Emirates 23

What principles exist for data processors? 24

- European Union 24
- China 25
- United States 25
- India 25
- Colombia 26
- United Arab Emirates 27

How are these principles enforced and what are the penalties for violators? 28

- European Union 28
- China 28
- United States 28
- India 29
- Colombia 30
- United Arab Emirates 31

Annex 1: Recent and ongoing reforms elsewhere around the world 32

Annex 2: Key definitions surrounding data privacy and security 33

Annex 3: Resources for worldwide data protection and privacy updates 36

References 37

Acknowledgements

NThis article was prepared by Lillyana Daza Jaller, Melissa Johns and Andre Lee of the Digital Impact Alliance (DIAL). Lex Mundi member firms Arthur Cox, JunHe LLP, Shardul Amarchand, Afridi & Angel, Brigard & Urrutia, and Michael Best provided review and comments for legal analysis relating to the European Union, China, India, United Arab Emirates, Colombia and the United States, respectively. We are grateful to Cristen Bauer for her review, updating and shepherding of this resource to publication.

Please note that this analysis summarizes the situation as of February 2019.

We would like to acknowledge our donors, the United States Agency for International Development (USAID), the Bill & Melinda Gates Foundation, and the Swedish International Development Cooperation Agency (Sida), for their vision and leadership in establishing DIAL and enabling our ongoing research agenda.

Disclaimer

The information provided in this paper does not, and is not intended to, constitute legal advice, but is for general informational purposes only. Information in this paper summarizes the situation as of February 2019 and may not constitute the most up-to-date legal or other information. This analysis should not take the place of tailored legal advice, and no reader should act or refrain from acting on the basis of information on this site without first seeking legal advice from counsel in the relevant jurisdiction.

License information

Background

Digital technologies have the potential to transform the way that governments and other service providers help citizens of low-income countries with healthcare, education and humanitarian aid. By harnessing the power of mobile, data analytics, and other technologies, resources can be more swiftly and cheaply deployed to the communities that need them most. By combining new data sources, such as private-sector data, with more traditional public sector datasets like census reports, technology can help governments to more effectively utilize their resources and deliver effective, efficient and sustainable development. DIAL's Data for Development (D4D) program of work aims to explore this type of program, supporting demonstration projects, investing in relevant capacity and platforms, and sharing learning and replicable implementation models.

While technology provides important new tools for tackling development challenges, the digital era also presents potential risks for governments, citizens, and international actors as they seek to understand issues of data protection, privacy, and security. New partnerships and ways of working have ushered in complex legal compliance issues, ethical concerns, and risk profiles.

The intersection of international development and technology paints a complex legal picture. For example, a UK data analytics firm might be funded by a Swedish donor in partnership with a development agency to help process Malawi health, census, and mobile phone data, in order to help provide data visualizations and insights that support the Malawi Ministry of Health to deploy better health services to citizens.

First, the multi-jurisdictional nature of this work creates a lot of uncertainty around the 'true legal liability' of various actors involved in the work or guidance for implementers seeking to understand how to follow the law. D4D operators often conduct business across many jurisdictions, including through funding arrangements; partner organizations; and implementing and on-the-ground activities, such as data processing, data hosting, or data transmission. In these cases, the D4D actors must be cognizant of the laws and policies of multiple countries as well as aware of how these policies apply to their work, and operation of the applicable law across jurisdictions may not be clear. Certainly, it is hard to find expert counsel willing and able to advise unequivocally in such cases.

Second, even within one jurisdiction, data protection and privacy and security laws governing this area of work are often unclear, hard to understand, or missing. Data protection and privacy laws often cross multiple areas of the law – for example, telecommunications, data privacy, or subject-specific legislation or regulation. For example, the United States still lacks a comprehensive piece of updated data protection and privacy legislation but, instead, has 'a jumble of hundreds of laws enacted on both the federal and state levels' (Gabel and Hickman, 2019). Additionally, data protection and privacy laws may be behind the pace of change of technology and evolving rapidly as governments attempt to keep up. Currently, 58 percent of countries globally have some form of data protection and privacy laws in place, with both developed and developing countries having similar levels of adoption (United Nations Conference on Trade and Development, 2019).[1]

Third, and finally, an added area of difficulty in the nexus between international development, technology, and law is that the technology itself can be confusing. Few lawyers are expert in both the technology and its application, with resulting impacts on the quality of both law and legal advice. As

[1] Currently 107 of countries have some form of data protection and privacy laws (of which, 66 are developing economies). This figure includes both countries in the process of updating outdated legislation, (i.e. the United States Privacy Act of 1974) and the 10 percent of countries with draft legislation on the books.

analytics applications become increasingly sophisticated, regulators in all jurisdictions will need to become increasingly technologically adept and ready to respond to new developments in the data space.

DIAL aims to support the D4D ecosystem by providing resources, such as this paper, that can help the various D4D actors (including governments, private sector firms, NGOs, and implementing partners) to better navigate the legal and regulatory environment around digital development and responsible data use.[2] This paper is an overview of data protection and privacy regulations from six jurisdictions, which can serve as a resource for regulators who are considering updates to their own data protection and privacy laws and as an illustration of the complexity in this fast-moving area.

[2] 'Responsible Data Use' is the collective duty to account for unintended consequences of working with data by (1) prioritizing people's rights to consent, privacy, security and ownership when using data in social change and advocacy efforts; and 2) implementing values and practices of transparency and openness.

Introduction

With the growth of personal data produced through mobile phone and internet use, and their consequent risks of misuse, regulators around the world are adopting stricter data protection regulations. The European Union's General Data Protection Regulation (hereinafter "GDPR") is one leading example in the field, and technology giants have already seen the effects of GDPR's enforcement (Romm, 2019a; Solon, 2018). Businesses are converging around European Union (hereinafter "EU") standards because it is operationally easier to peg to the higher standards than differentiate across jurisdictions and it is also not worth the risk of paying high fines for failure to comply (Greenleaf, 2018). To oversee enforcement of GDPR, governments are also increasing personnel in relevant agencies as they begin to tackle emerging data protection issues (European Data Protection Board, 2019; Government of Colombia, 2018).

For regulators seeking to update their own laws addressing data protection, privacy, and security, this paper compares some central elements of current legal regimes in the EU, China, Colombia, India, United Arab Emirates, and the United States. The countries covered in this paper were chosen to represent a range of approaches, geographic locations, development levels, and legal origins. Annex 1 also highlights a few recent and ongoing reforms being implemented elsewhere by various other countries around the world.

This paper looks at examples of recent privacy and data protection legislative reforms, as well as provides a response to questions often raised by regulators when considering updates to their legislation, such as:

- What are global legal standards for processing and securing personal data?
- What principles underlie the more detailed regulations?
- How are these regulations enforced across the countries compared?
- How do the definitions of key terms differ – perhaps intentionally – across jurisdictions?

This paper is divided into four sections. **Section one** analyses the global legal standards for processing personal data, noting the different regulatory approaches among the various jurisdictions that were studied. **Section two** lays out security requirements for processors and controllers when handling personal data. **Section three** identifies the overarching principles underlying data protection and privacy regulations. Finally, **section four** looks at enforcement mechanisms and penalties for violations of data protection and privacy regulations.

This paper is not intended to be exhaustive or replace any of the other guidance materials available or the regulations themselves. Rather, it seeks to highlight some commonalities and differences across several jurisdictions as a resource and starting point for national lawmakers and experts as they begin undertaking reforms to their own data protection and privacy laws. As such, there are three additional resources annexed at the end of the paper. Annex 2 contains a table comparing some of the key terms and definitions found in the various pieces of legislation analyzed in this paper, allowing the reader to note how countries differ in the way they approach important terms related to data protection. Finally, Annex 3 highlights a few helpful, free databases and resources for readers to keep up to date on the latest data protection and privacy developments around the world.

What are global legal standards for processing personal data?

European Union

The *Regulation (EU) 2016/679,* also known as the GDPR, applies to any organization operating within the EU or any organization outside of the EU that offers goods or services to customers or businesses in the EU or monitors the behavior of individuals in the EU (Regulation (EU) 2016/679 General Data Protection Regulation [GDPR], 2016, Art. 3). Due to the EU's importance in global markets, many businesses started preparations to comply with the GDPR well before its May 25, 2018 implementation date (IAPP-EY, 2018).

Under the terms of the GDPR, organizations must ensure that personal data is gathered legally and under strict conditions. Those who collect and manage it are obliged to protect it from misuse and exploitation, as well as to respect the rights of data subjects. If they don't, they face significant penalties.

The GDPR applies to both "controllers," who "determine the purposes and means of the processing of personal data", and "processors," who are responsible for "process[ing] personal data on behalf of the controller". For example, a company wishing to engage with its customers through email would be the controller, while the email-marketing firm hired to do the work would be the processor. The GDPR requires processors and controllers to maintain records of personal data and processing activities and makes them both legally liable if a breach occurs. Controllers are obliged to ensure that the organization processing personal data on their behalf complies with the GDPR and is responsible for any security problems that occur. Specifically, under Article 28, the GDPR states that the controller must,

> (1) Choose a data processor that provides "sufficient guarantees" about its security measures;
> (2) Have a written contract requiring the processor, among other requirements, to undertake the same security measures that the controller would have to take if it were doing the processing itself; and,
> (3) Ensure the processor makes available all information necessary to allow the controller to demonstrate compliance, which may include allowing the controller or an authorized third party to audit and inspect the processor (GDPR, 2016, Art. 28).

Processors can help ensure compliance with security obligations. If a controller lacks the resources or technical expertise to implement certain measures, it should consider engaging a processor that can ensure personal data is processed securely.

Personal Data

The GDPR applies to "the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system" (GDPR, 2016, Art. 2(1)).

Personal data only includes information relating to natural persons who can be identified or are identifiable directly or indirectly from the information in question or from that information in combination with other information (GDPR, 2016, Art. 4(1)). Personal data may also include special categories of personal data or criminal conviction and offenses data (GDPR, 2016, Art. 9-10). These are considered to be more sensitive and may only be processed under limited circumstances. Pseudonymisation of data can help reduce privacy risks by making it more difficult to identify individuals, but the data is still considered personal data.

Anonymized Data

Anonymized data "does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable" (GDPR, 2016, p.5 (26)). If personal data can be truly anonymized, then the anonymized data is not subject to the GDPR. However, the Article 29 Data Protection Working Party (Working Party) published an opinion on anonymization techniques which cautioned that removing "directly identifying elements" is not anonymization (Article 29 Data Protection Working Party [Working Party], 2014).[3]

A dataset is anonymized only if it has none of the following properties:

- Singling out: some or all of the records which identify a data subject may be isolated
- Linkability: two or more records concerning an individual or group in the dataset(s) may be linked
- Inference: an attribute may be deduced "with significant probability" from a group

Thus, choosing an optimal anonymization technique should be decided on a case-by-case basis that ideally meets the following three criteria: (1) no singling out of an individual; (2) no linkability between records relating to an individual; and (3) no inference concerning an individual (Working Party, 2014, p.23-4). **Figure 1** uses these three criteria to compare the strengths and weaknesses of several anonymization techniques (Working Party, 2014, p.24).

Figure 1 – Strengths and weaknesses of anonymization techniques

	Is Singling out still a risk?	Is Linkability still a risk?	Is Inference still a risk?
Pseudonymisation	Yes	Yes	Yes
Noise addition	Yes	May not	May not
Substitution	Yes	Yes	May not
Aggregation or K-anonymity	No	Yes	Yes
L-diversity	No	Yes	May not
Differential privacy	May not	May not	May not
Hashing/Tokenization	Yes	Yes	May not

Source: Working Party 29 Opinion on Anonymization Techniques

Helpfully, the Working Party includes "good anonymization practices" in its opinion (Working Party, 2014). Additionally, other enforcement agencies around the world have provided guidelines in this regard (Personal Data Protection Commission, 2018).

Pseudonymization techniques, such as hashing or tokenization, change one attribute in a record to avoid the data subject being identified indirectly (Working Party, 2014). Noise addition is when certain attributes in a dataset are modified to decrease their accuracy, without changing the overall distribution. Substitution, one of the "randomization" techniques, is similar to noise reduction, in that an attribute in a dataset is replaced by another. Another randomization technique, differential privacy, is where a data controller creates two datasets: one anonymized version that can be shared, and an original (Working Party, 2014). Aggregation and K-anonymity are techniques whereby the subjects' attributes are generalized to the point where one cannot be singled out. L-diversity takes this a step further, by changing the attribute values in each equivalence class, thereby preventing the threat of inference (Working Party, 2014).

[3] The Article 29 Working Party was an independent advisory body on data protection. On May 25, 2018, it was replaced by the European Data Protection Board (EDPB) according to the GDPR.

Lawful basis for processing

Under the GDPR, consent is one of six lawful bases for processing personal data. The GDPR defines consent as, “any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her” (GDPR, 2016, Art. 4(11)). Consent is treated as an ongoing and actively managed choice, and not simply a one-off compliance box to tick and file away. In practice, this encourages clear and more granular opt-in methods, good records of consent, and simple easy-to-access ways for people to withdraw consent (Information Commissioner’s Office, 2012).

The other five lawful bases for processing set out in Article 6(1) GDPR are:

- **Contract:** The processing is necessary for a contract with the data subject or the data subject has requested specific steps to be taken before entering into a contract.
- **Legal obligation:** The processing is necessary for the data controller to comply with EU or member state law.
- **Vital interests:** The processing is necessary to protect someone’s vital interests.
- **Public task:** The processing is necessary for the data controller to perform a task in the public interest or in the exercise of official authority vested in the data controller.
- **Legitimate interests:** The processing is necessary for the legitimate interests of the controller or those of a third party, unless the data subject’s interests or fundamental rights and freedoms override those legitimate interests. Non-public bodies may rely on this lawful basis. However, it does not apply to public authorities processing data to perform official tasks.

Additionally, processing sensitive data is prohibited unless one of the ten lawful bases from Article 9 of the GDPR is met. This means that in order to process sensitive data, you must have a lawful basis under both Article 6 and Article 9 of the GDPR. The lawful bases under Article 9 of the GDPR are:

- **Explicit consent**: Unfortunately, no explanation is given as to how explicit consent differs from consent.
- **Employment or social security and social protection law**: The processing is necessary for the purposes of obligations under employment or social security and social protection law.
- **Vital interests**: The processing is necessary to protect someone’s life where that person is physically or legally incapable of giving consent.
- **Foundation, association or not-for-profit**: The processing is carried out in the course of the legitimate activities of a foundation, association or any other not-for-profit body with a political, philosophical religious or trade union aim where the processing solely relates to members.
- **Public data**: The processing relates to personal data which are manifestly made public by the data subject.
- **Legal claims**: The processing is necessary for the establishment, exercise or defense of legal claims.
- **Public interest**: The processing is necessary for reasons of substantial public interest on the basis of EU or member state law.
- **Healthcare**: The processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems or services.

- **Public health**: The processing is necessary for reasons of public interest in the area of public health on the basis of EU or member state law.
- **Archiving, research or statistical purposes**: The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes on the basis of EU or member state law.

Processing of personal data relating to criminal conviction and offence is only lawful where carried out under the control of an official authority or when the processing is authorized by EU or member state law pursuant to Article 10 of the GDPR.

China

China's principal data protection law is the *Cybersecurity Law of the People's Republic of China* (hereinafter "CSL"), which applies to any entity that provides services online (Ning and Wu, 2019).

Data protection in China is also impacted by various other laws, standards, and decisions. The *General Rules of Civil Law* promulgated in 2017 and set the principle that entities or individuals shall not illegally collect, use, process or transmit the personal data of others, or illegally buy or sell, provide or make public the personal data of others. The following major laws and regulations also contain protection provisions regarding personal data:

- The *Consumer Rights and Interests Protection Law* revised in 2013 includes provisions on the protection of consumers' personal information.
- The *Provisions on Protecting the Personal Information of Telecommunications and Internet Users* (hereinafter the "Personal Information Provisions") were issued in 2013, and they regulate the collection and using of personal information by telecommunication service providers.
- The *Amendment IX* to the *Criminal Law* issued in 2015 provides the criminal liabilities for personal information related crimes.
- The 2018 *Information Technology-Personal Information Security Specification* (hereinafter "the Standard") provides detailed explanations and practical guidance to public or private data controllers about the collection, preservation, use, sharing, transfer, public disclosure and other personal information processing activities.

The Standard falls under one of the CSL's six systems, the "personal information and important data protection" system" (Sacks, 2018). Its introduction followed discussions among the Chinese government and the private sector about how to approach data privacy protections and the public's increasing concern of their rights about their personal data (Sacks, 2018).

It is important to note that standards in China are not legally binding and merely serve as guidelines for compliance reviews by the government. The Standard should therefore be viewed as the government's indication of good practice and perhaps future lawmaking direction, but not a required set of measures for firms to adopt (Sacks, 2018).

Personal Data

The definition and scope of personal sensitive information in China is broader than the GDPR. Personal data is defined in Article 4 of the Personal Information Provisions and Article 76(5) of the CSL and refers to:

> All kinds of information, recorded electronically or through other means, that taken alone or together with other information, is sufficient to identify a natural person's identity, including but not limited to natural persons' full names, birth dates, national identification numbers, personal biometric information, addresses, telephone numbers, and so forth (translated in Creemers, Trilolo, and Webster, 2018).

An annex to the Standard provides a list of examples of "personal information", including IP addresses and website tracking records. Section 3(2) of the Standard further defines "sensitive" personal data as "the personal data that, if divulged, illegally disclosed, or abused, can harm personal or property safety, or can easily result in the damage of reputation, physiological as well as psychological health, or cause the person to be discriminated against." Furthermore, Appendix B of the Standard defines data such as email address, personal phone number and residential information as sensitive, which is not the case with the GDPR.[4]

Lawful basis for processing

The CSL and the Personal Information Provisions set the principle that when collecting or using personal information, the service providers shall clearly inform the users of the purposes, methods and scope of information collection or use, the channels for the users to inquire about and correct information and the consequences of refusing to provide information. Further, the Standard requires that processors "de-identify" personal data before they share it, unless they obtain informed consent from the data subject. In this respect the Standard is stricter than GDPR, which does not require consent prior to sharing data. However, both recommend risk assessment measures prior to sharing.

While the CSL does not allow for any exceptions to consent, the Standard includes several exceptions similar to those of the GDPR, including national security; public and personal interest; and contractual obligations, and others that diverge from the GDPR, such as troubleshooting goods and services and reporting news agencies. The Standard also requires that data processors differentiate based on the intended purpose of collection and use of personal information, whether it be for the provision of core services or non-core or add-on services. For example, a business would need to identify the core purposes and ancillary purposes for its collection of sensitive personal information and obtain separate consent for each item of sensitive personal information that is collected for ancillary purposes. If any data processing activity goes beyond the scope of the original consent, the data subject must provide separate consent. Businesses are entitled to decline to provide additional services if they don't obtain the data subjects' express consent to the ancillary uses of their personal data.

Additionally, whereas the GDPR allows data processors to withhold information from a privacy notice so long as it can be accessed elsewhere, the Standard provides the specific information that must be included in the notice, including data subjects' rights; complaint handling; security principles followed; and controller's contact information. Finally, the Standard requires that data subjects be notified of the cessation of data processing.

United States

At the national level, the United States does not have a comprehensive data protection policy, offering a more hands-off approach to data privacy than other developed economies. It has a general federal consumer protection law and a series of sector-specific federal laws regulating financial, health, and

[4] *See* GDPR (2016) Art. 9.

children's online privacy (Chabinsky and Pittman, 2019, Sec. 1(1)-1(3)). In recent months—mainly as a result of high-profile data breaches—there has been talk of a federal data protection law, with support from the tech industry as well as state representatives (Temple-Raston, 2018).

Chabinsky and Pittman (2019) provide a detailed list of the general and sector specific legislation that impacts data protection in the United States. The most relevant federal laws to data privacy and security are:

- The *Federal Trade Commission Act* (hereinafter "FTC Act"): Section 5 regulates unfair and deceptive practices and has been interpreted to apply broadly to privacy and security representations made to consumers.
- The *Health Insurance Portability and Accessibility Act* (hereinafter "HIPAA"): Governs the use and disclosure of certain types of health information by covered entities, which include healthcare providers and health plans, and outlines privacy and data security standards and data breach notification procedures for these types of entities.
- The *Gramm-Leach-Bliley Act* (hereinafter "GLBA"): Imposes privacy restrictions and information security requirements on financial institutions. Separately, major payment card brands, through their participation in the Payment Card Industry Security Standards Council, require compliance with the Payment Card Industry Data Security Standard (PCI DSS), an information security standard, for merchants to accept payment cards.
- The *Children's Online Privacy Protection Act* (hereinafter "COPPA"): Regulates children's online privacy by requiring websites, mobile applications and other online services that knowingly collect information from children under age 13 or that are targeted toward such children to make certain disclosures and obtain verifiable parental consent before collecting and using personally identifiable information obtained from children.

In addition, individual states are passing more comprehensive privacy protections. In 2004, California passed the *California Online Privacy Protection Act* (CalOPPA), which requires websites to feature a conspicuous privacy policy stating exactly what information is collected and with whom it is shared. In 2005, it passed the *Shine the Light Law*, which requires companies to disclose, upon the request of a California resident, what personal information has been shared with third parties for marketing purposes, as well as the parties with which the information has been shared. Most recently, the *California Consumer Privacy Act,* which goes into effect in 2020, grants data subjects stronger rights with regard to their data collected by businesses and also subjects violators to penalties. In certain circumstances it also provides a private cause of action and statutory damages to those who have suffered a data breach. This places companies at a risk for class action litigation, which can be very costly and time-consuming.

Most recently, the Washington State Senate passed the *Washington Privacy Act*, which adopts many elements of the GDPR (Senate Bill 5376 Protecting Consumer Data, 2019). If approved by the House of Representative, the Act will grant consumers the right to access their data gathered by companies, and to request the correction of inaccurate data and compel data controllers to conduct risk assessments. It restricts the use of facial recognition technology by companies and prohibits its use by public agencies. Any violations of the Act would be enforced under the state's *Consumer Protection Act*.

Given the patchwork of laws currently in force in the United States, many – including the heads of large tech companies – are calling for a federal privacy regulation (Farrell, 2019). This holds promise for setting one national standard for data privacy protection.

Personal Data

The FTC Act does not define personal data; however other laws have specific rules for certain personal information. The GLBA defines non-public personal information (NPPI) as personally identifiable financial information that a financial institution collects about an individual in connection with providing a financial product or service, unless that information is otherwise publicly available. The GLBA requires financial institutions to comply with certain privacy provisions with respect to NPPI and to safeguard NPPI. Moreover, certain regulations require that financial entities notify the regulators in case of data breach affecting sensitive customer data (Jolly, 2018).

In addition, the *Fair Credit Reporting Act* regulates the collection, use, and disclosure of consumer reports (Jolly, 2019). Credit reports and credit scores are a form of consumer reports. HIPAA regulates Personal Health Information (PHI), which is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. HIPAA has both privacy and security rules that regulate the disclosure and protection of PHI, respectively. HIPAA also requires written consent of a data subject prior to disclosure of psychotherapy notes by a regulated entity.

There are also 50 state data breach laws that generally protect personal data from disclosure to unauthorized third parties. The definition of personal data can vary state to state but is generally a person's name in combination with a piece of sensitive information such as social security number or financial account number with a means to access that financial account.

Lawful basis for processing

As opposed to regulations in other countries that contain the concept of consent when disclosing personal data, the FTC Act does not address consent but rather regulates personal data based on whether disclosure may be perceived to be unfair or deceptive (Jolly, 2018). Section 5 of the FTC Act generally permits "implied consent" to a company's privacy policies to be sufficient, where assent to that company's practices is inferred from the consumer's behavior. That is, if the consumer uses a service that has published certain privacy practices in a sufficiently transparent manner, the consumer is deemed to have consented to those practices.

Only in certain circumstances does the FTC recommend "affirmative express consent"—robust notice and some explicit act by the consumer—before information can be collected. This is expected if the company uses the consumer's data in a manner that is materially different than what it was originally collected for or when collecting "sensitive data," which encompasses relatively few categories in the U.S. context (e.g., information about children, financial and health information, and precise geolocation information).

According to COPPA, which is enforced by the FTC, verifiable parental consent is required for websites aimed at children or websites that gather personal data from children before that data is shared with third parties (Jolly, 2018). Under GLBA, financial institutions must notify data subjects of their privacy policy at the beginning of their relationship and every year thereafter, allowing the customers to opt-out of certain disclosures of their personal data (Jolly, 2018). Finally, HIPPA requires written consent of a data subject prior to disclosing personal data.

In 2017, Congress introduced a new law, eliminating a requirement that broadband providers obtain consent prior to collecting data about their customers' online activities, such as their browsing history (Public Law 115–22, 2017). This nullified a rule introduced by the Federal Communications Commission in 2016, which ordered internet service providers (ISPs) to comply with certain data privacy requirements, including obtaining affirmative consent prior to using or disclosing their customer's confidential information (Federal Communications Commission, 2016).

India

India currently does not have a national data protection law. Seeking to introduce a comprehensive data protection framework, the Ministry of Electronics and Information Technology (hereinafter the "MeitY") released a draft of the *Personal Data Protection Bill, 2018* in 2018 (hereinafter the "PDP Bill") (Personal Data Protection Bill, 2018 [PDP Bill], 2018). As of September 2019, the PDP Bill is under inter-ministerial consultation and has not yet been tabled in the Parliament.

In 2018, in a landmark judgement—the Indian Supreme Court ruled the right to privacy is a "fundamental right" (Justice K.S. Puttaswamy (Retd) vs Union of India, 2018).[5] The right to privacy specifically includes "information privacy", which is the right to exercise control over the collection, use, and dissemination of one's personal data.

Currently, there are two main pieces of legislation providing rules for data security and privacy in relation to processing of personal data (Subramaniam and Subramaniam, 2019):

- The *Information Technology Act* 2000, amended by the *Information Technology (Amendment) Act*, 2008 (2008) (hereinafter the "IT Act") (Information Technology Act, 2008 [IT Act], 2008); and
- The *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules* 2011 (hereinafter the "IT Rules") (Information Technology Rules, 2011 [IT Rules], 2011).

The IT Rules prescribe compliance for body corporates related to the collection, disclosure, and transfer of personal information and sensitive personal data. However, the IT Rules only apply to processing of data of individuals located in India, limiting their scope. Furthermore, a *Clarification on the Privacy Rules*, issued by the former Ministry of Communications and Information in 2011, (now the MeitY) excludes Indian outsourcing service providers who provide services related to the collection, storage or handling of personal information from the collection and disclosure information requirements if they are under contractual obligation with any legal entity located within or outside India. In other words, the obligations under the IT Rules only apply to companies collecting personal data from an individual, for the purpose of directly providing a service to that individual. Finally, several sectoral laws address data confidentiality, particularly with regard to healthcare, telecommunications, banking, and other financial services (Subramaniam and Subramaniam, 2019, Sec. 1(2) and 1(3)).

Personal Data

[5] In a landmark judgement, the Supreme Court unanimously held that the Right to Privacy is a fundamental right under Art. 21 of the Constitution of India. The case was brought by a retired high court judge who challenged the government's proposed Aadhaar scheme for a uniform biometric based identity system for all Indians. Under the scheme, a unique 12-digit code would be generated for every person and registration would be a mandatory condition in order to avail certain privileges (e.g. filing taxes, opening bank accounts, getting loans, etc.) See also, Wilmap (2017).

The IT Rules define personal information as “any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person” (IT Rules, 2011, Rule 2(i)). However, current Indian laws are comparatively less broad than other models, as the law governs only “body corporates” and many of the obligations only pertain to “sensitive information”. According to the IT Act, a body corporate is any “firm, sole proprietorship or other association of individuals engaged in commercial or professional activities” (IT Act, 2008, Art. 43A(i)). Sensitive personal data is defined by the IT Rules as personal data relating to the following (IT Rules, 2011, Rule 3):

- Password,
- Financial information,
- Physical, physiological and mental health condition,
- Sexual orientation,
- Medical records and history,
- Biometric information,
- Any detail relating to the above items as provided to a body corporate for providing a service, and
- Any of the information received under the above clauses by a body corporate for processing, stored or processed under lawful contract or otherwise.

Lawful basis for processing

In the case of personal information, there is no requirement for obtaining consent to collect data, or for disclosure of that information to a third party. Each organization that collects that data must have a privacy policy, however, which should mention what data is collected and for what purpose (IT Rules, 2011, Rule 4). In the case of sensitive personal data, consent by the provider of information is required before information can be collected, and consent is defined as “in writing, through letter or Fax or email” (IT Rules, 2011, Rule 5(1)).

Organizations must provide the following information to subjects while collecting sensitive data (IT Rules, 2011, Rule 5(3)):

- The fact that the data is being collected
- The purpose for which the data is being collected
- The intended recipients of the data
- The name and address of the agency collecting the information and the agency that will retain the information

Notably, the IT Act does not apply to:

- Personal information or data stored in a nonelectronic medium
- Any information that is freely available or accessible in the public domain
- Any information furnished under a law for the time being in force (compliance with a legal obligation, demanded by government mandate for an investigation, etc.)

Grounds of Processing

The IT Rules also provide that information collected shall only be used for the purpose for which it has been collected and should not be retained for longer than is required for those purposes for which the information may lawfully be used or required under any other law for the time being in force (IT Rules, 2011, Rule 5(4)(5)). Further, sensitive personal data will only be collected if necessary, for the lawful purpose connected with the function and activity of a body corporate (IT Rules, 2011, Rule 5(2)(b)).

Disclosure and Transfer

Disclosure of sensitive personal data requires prior consent, or the presence of a legal obligation to disclose (IT Rules, 2011, Rule 6). For transfer of sensitive personal data, the third party to whom data is transferred should ensure equivalent levels of data protection. In addition, there should either be consent from the data provider or a contractual necessity justifying such transfer.

Aadhaar – A Digital Identification Project

Aadhaar, which means "foundation" in Hindi and other Indian languages, is the first foundational ID issued by the government of India. Those who sign up for an Aadhaar number—a unique, randomly generated string of 12 digits—must have their faces photographed, fingerprints taken, and irises scanned. The system also includes a publicly available interface, or open API, that allows any licensed service provider to verify if users are who they claim to be. In the seminal 2018 judgment mentioned above, the Supreme Court of India held that the mandatory use of Aadhaar by private parties for verification of identity was in contravention of the right to privacy granted to each citizen (Justice K.S. Puttaswamy (Retd) vs Union of India, 2018). However, the *Aadhaar and Other Laws (Amendment) Act,* 2019 enacted in July 2019 allows private parties to use Aadhaar for physical or electronic verification if people voluntarily part with their Aadhaar details (Aadhaar and Other Laws (Amendment) Act, 2019, 2019). On the basis of this ordinance, people can use Aadhaar to open bank accounts, buy SIM cards, and receive entitlements from the government.

Personal Data Protection Bill

The proposed draft PDP Bill specifies more stringent grounds for data processing (Coos, 2019; PDP Bill, 2018). There are separate consent standards for personal data and sensitive personal data, which are compared in **Table 1** below (PDP Bill, 2018). Personal data can only be processed (PDP Bill, 2018, Sec. 12-17):

- on the basis of consent,
- for functions of the State,
- in compliance with law,
- if necessary for prompt action,
- for purposes related to employment, or
- other reasonable purposes as specified.

As opposed to the GDPR's "legitimate interests" grounds, where the data controller can determine what constitutes reasonable purposes, the PDP Bill's "reasonable purposes" provision requires that the Data Protection Authority (DPA) specify the grounds (PDP Bill, 2018, Sec. 17).[6] The PDP Bill lists several grounds that may be specified, including information security and processing of publicly available personal data. Additionally, the DPA must provide adequate safeguards to ensure the protection of data

[6] For a detailed comparative analysis of the draft PDP Bill and the GDPR, see Deloitte PDPB v. GDPR (2019).

subjects' rights. The grounds for processing sensitive personal data are even more limited, requiring "explicit consent" from the data subject.

Table 1 – Consent requirements under the Indian Personal Data Protection Bill

Consent (for personal data)	**Explicit** consent (for sensitive personal data)
Free (as under the standard in contract law – no fraud, coercion etc)	**Free** (as under the standard in contract law – no fraud, coercion etc)
Informed with adequate notice	**Informed** on the purposes of processing that may have significant consequences for the data principal
Clear with defined scope of processing	**Clear** within the context
Specific, in terms of whether data principal can determine scope of consent for processing	**Specific** for each use of different categories of sensitive data for processing
Capable of being withdrawn	Capable of being withdrawn

Source: Author's from the PDP Bill (2018)

Colombia

Data protection is a relatively new topic in Colombia, and the interpretation of data protection on the books is still being shaped. Colombia is notable in that its legislation is not limited to the data processing carried out in Colombia by the private sector but is equally applicable to the processing performed by public-sector entities (Adarve and Acosta, 2017).

Data privacy rules in Colombia are found throughout an array of legal instruments. The Constitution provides individuals the right to privacy and to data rectification. *Law 1266 of 2008* regulates this right with regard to data subject rights in relation to credit history reporting and consultation with credit bureaus. *Law 1273 of 2009* criminalized unlawful and unauthorized processing of personal data. *Law 1581 of 2012*, and its *Decree 1074 of 2015* provide the most comprehensive rules regarding data protection, protecting data subjects residing in Colombia or whose personal data is stored or processed in Colombian territory (Adarve and Acosta, 2017). Additionally, decrees and circulars lay out other rules, including the registration of data controllers and adequacy standards for transborder data flows.

Personal Data

While Colombia defines controllers, processors and personal data in essentially the same way as the GDPR, it classifies personal data into the following subcategories outlined in **Table 2** below.

Table 2 – Relevant data protection definitions in Colombia

Public Data	**Data that is, by exclusion, not semi-private, private or sensitive. It includes, but is not limited to, the following:** • **Civil status of any person** • **Profession or trade** • **Capacity as entrepreneur or public servant** **It may be contained in, but not limited to, the following:** • **Public records**

	• **Public documents** • **Official gazettes and bulletins** • **Duly executed and nonconfidential judicial decisions**
Private Data	Data that is only relevant for the data subject (i.e., the individual whose personal data is the subject of the processing), regarding its intimate or secretive nature.
Semi-Private Data	Data that has no intimate, reserved or public nature, and whose knowledge or disclosure may be of interest not only to the data subject, but to a certain sector or group of persons or to society in general, such as financial data or credit for business or services.
Sensitive Data	Data affecting the intimacy of the data subject or misuse of which may lead to the discrimination of the data subject, such as disclosing the data subject's racial or ethnic origin, political orientation, religious or philosophical convictions, union membership or membership in social or human rights organizations, or in any other organization promoting the interests of any political party or guaranteeing the rights and guarantees of opposing political parties, as well as any data related to the health, sex life and biometrical information of the data subject.

Source: Author's from Law 1581 of 2012, and its Decree 1074 of 2015.

Colombia's *Law 1581 of 2012* does not apply to databases that are (DLA Piper (2019a)):

- Kept exclusively in a personal or domestic sphere, unless supplied to third parties without previously requesting and obtaining informed consent from the data subject,
- Purposed toward national security and defense, as well as the prevention, detection, monitoring and control of money laundering and terrorism financing,
- Related to or containing intelligence and counterintelligence information,
- Containing journalistic information and other editorial content,
- Regulated by Law 1266 of 2008, related to data protection in the financial and credit sector, particularly for credit and scoring agencies,
- Regulated by Law 79 of 1993, related to population census.

Lawful basis for processing

The Colombian data protection regime uses the expression "authorization" to refer to consent. It is defined as "prior, express, and informed" consent, freely granted by the data subject to carry out the processing of personal data. The Constitutional Court defined the qualities that legitimize the processing of personal data as outlined in **Table 3**.

Table 3 – Constitutional Court of Colombia's definition of authorization (*consent*)

Prior	**Consent must be provided in a stage before data is even collected.**
Express	Consent shall be unequivocal. There is *no* implied consent. However, in addition to written and oral consent, consent may be given through the unequivocal conduct of the data subject. Such conduct must reasonably and evidently demonstrate authorization.
Informed	The data subject must be fully aware of the effects of their consent.

Free	Consent is freely given by the data subject. This definition is rather unhelpful because it uses the term itself to define the term. It probably means a lack of coercion and/or duress.

Like the GDPR, Colombian case law provides exceptional circumstances where personal data can be processed without prior consent:

- When the data is required by a public or administrative agency during the exercise of its legal duties or by a legal order,
- Public data,
- Health or sanitary emergencies,
- Historical, statistical or scientific purposes,
- When the data is related to the Civil Registry.

Colombia requires controllers to adopt a data protection policy to ensure compliance with its data protection regime, recorded in physical or electronic media format, written in clear and simple language, and disclosed to the data subject. The data subject must be given timely notice of any substantial change to such policies, and if the processing changes, the controller must obtain consent again.

United Arab Emirates

In the United Arab Emirates (hereinafter "UAE"), there is no general federal data protection law. Several emirate-specific regulations, penal codes, and articles in the UAE Constitution do, however, provide guidance and standards for data regulation. Article 31 of the UAE Constitution establishes a general right of "freedom of communication by means of the posts, telegraph or other means of communication and their secrecy shall be guaranteed in accordance with the law" (UAE Constitution 1971, 2004). Notably, this only applies to citizens of the UAE, who only make up around 11% of the total population living in the country (Global Media Insight, 2019). The rest of the country is comprised of expatriates, primarily from India, Pakistan, Egypt, and the Philippines.

In addition, the Dubai International Financial Centre (DIFC) and the Abu Dhabi Global Market (ADGM) zones have rules and regulations that apply to those specific areas. In the ADGM, the Board of Directors enacted a series of regulations concerning the processing of personal data in an exercise of its powers under Article 6(1) of *Law No. 4 of 2013* issued by His Highness the Ruler of the Emirate of Abu Dhabi. In the DIFC, the *DIFC Data Protection Law No. 1 of 2007* prescribes rules and regulations regarding the collection, handling, disclosure and use of personal data in the DIFC, the rights of individuals to whom the personal data relates, and the power of the Commissioner of Data Protection in applying the Data Protection Law (DIFC Data Protection Law No. 1 of 2007 [DIFC Data Protection Law], 2018). The DIFC Data Protection Law is consistent with EU regulations and OECD guidelines. The ADGM Board of Directors regulations and the DIFC Data Protection Law provide the same data protection regulations.

Personal Data

Article 378 of the *Penal Code*, established in 1987 under *Federal Law 3*, provides that the publication of any personal data related to an individual's private or family life is an offense. It outlines the possibility of sanctions of imprisonment and/or a fine for anyone who publishes news, pictures or comments pertaining to secrets of a person's private life. Corporations and individuals can be found guilty of this

violation. In addition, there are no special rules for certain types of personal data, such as public data, private data, semi-private data, or sensitive data.

In both the ADGM and the DIFC, personal data is defined as any data referring to an "Identifiable Natural Person". An "Identifiable Natural Person" is a "natural living person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his biological, physical, biometric, physiological, mental, economic, cultural or social identity" (DFIC Data Protection Law, 2018, p.32). Sensitive personal data is defined as "personal data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership and health or sex life" (DFIC Data Protection Law, 2018, p.33).

Lawful basis for processing

In the ADGM and the DIFC, personal data may only be processed if the data subject has given his written consent to the processing of that personal data. Sensitive personal data may only be processed if the data subject has given an additional written consent to the processing of that specific data. Data subjects also have the right to object, on reasonable grounds, at any time to the processing of personal data, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing.

Controllers may only process personal data if (DFIC Data Protection Law, 2018, Art. 9):

1) The data subject has given his written consent to the processing of that personal data,
2) Processing is necessary for the performance of a contract to which the data subject is party,
3) Processing is necessary for compliance with any regulatory or legal obligation to which the data controller is subject,
4) Processing is necessary in order to protect the vital interests of the data subject,
5) Processing is necessary for the performance of a task carried out in the interests of the ADGM or in the exercise of the ADGM's Board of Directors' functions or powers vested in the data controller or in a third party to whom the personal data are disclosed,
6) Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by the third party to whom the personal data are disclosed, except where such interests are overridden by compelling legitimate interest of the data subject.

Controllers may NOT process sensitive personal data unless (DFIC Data Protection Law, 2018, Art. 10):

1) Processing is necessary for the purposes of carrying out the obligations and specific rights of the data controller,
2) Processing is necessary to protect the vital interests of the data subject,
3) Processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed to a third party without the consent of the data subjects,
4) The processing relates to personal data which are manifestly made public by the data subject, or is necessary for the establishment, exercise or defense of legal claims,
5) Processing is necessary for compliance with any regulatory or legal obligation to which the data controller is subject,

6) Processing is necessary to comply with any regulatory, auditing, accounting, anti- money laundering or counter terrorist financing obligations that apply to a data controller or for the prevention or detection of any crime,
7) Processing is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of healthcare services, and where those personal data are processed by a health professional subject under law or rules established by competent bodies to the obligation of confidence or by another person subject to an equivalent obligation.

Exemptions:

Under *Article 337 of the Penal Code*, which applies to the UAE as a whole, the requirement to obtain the individual's written consent can be waived where both: a UAE official/public authority has required the transfer of data to it, and the transfer serves public interests or national security.

In the ADGM and the DIFC, the regulations for processing sensitive personal data do not apply if a permit has been obtained from the Registration Authority (ADGM) or the Registrar of Companies (DIFC) to process sensitive personal data, or if the data controller applies adequate safeguards with respect to the processing of the personal data. The Registrar of Companies in the DIFC was appointed pursuant to Article 7 of the *Companies Law, DIFC Law No. 2 of 2009*. The Registrar and the Registration Authority are responsible for all matters related to the incorporation and registration of companies in the DIFC and ADGM, respectively. The ADGM Board of Directors may also make rules exempting data controllers from compliance with these regulations or any parts of these regulations. In both DIFC and ADGM, persons who hold and handle sensitive data are required to register as data controllers, to report transfers of data, and to undertake not to handle data improperly.

What are global legal standards for securing personal data?

European Union

The GDPR does not espouse a legal standard for securing personal data. It does not define the security measures that should be in place and understands that there is no one-size-fits-all solution. Instead, a key principle of the GDPR is that personal data is processed securely by means of "appropriate technical and organizational measures," known as the "security principle" (GDPR, 2016, Art. 32(1)). At a minimum, proper security requires the consideration of things such as risk analysis, organizational policies, and physical and technical measures (e.g. pseudonymization and encryption). What measures will be appropriate should take into account the costs of implementation, and the nature, scope, context and purpose of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Measures must ensure the "confidentiality, integrity availability and resilience" of the organization's systems and services as well as the ability to restore access to personal data in the event of an incident (GDPR, 2016, Art. 32(1)(b)).

China

China has a tiered system for data protection. Under the Multi-Level Protection Scheme, the Personal Information Provisions requires the telecommunication or internet service providers take the following measures to secure personal data (translated in Creemers, 2013):

- Specify the responsibility of each department and branch in terms of managing the security of users' personal information,
- Establish work processes and security management systems for the collection and use of users' personal information,
- Manage the authority of different staff members and agents, review the batch export, duplication and destruction of information, and take measures to prevent the leakage of confidential information,
- Properly keep the carriers recording users' personal information,
- Conduct access inspection of the information system that stores users' personal information, and take intrusion prevention, anti-virus and other measures,
- Record the staff members who perform operations of users' personal information, the time and place of such operations, and the subject matter, etc,
- Carry out communications network security protection work as required by the relevant authority.

Telecommunication and internet service providers who violate the above rules may be warned by authorities and imposed monetary fines, or where the situation is serious, be pursued for criminal liability.

In addition, the Ministry of Public Security will classify entities based on certain factors, including the service offered, the types of data processed, and the potential impact of a security incident, particularly on national and economic security. Entities that are classified as posing high risks are subject to stricter security requirements, such as regular monitoring; reporting incidents to the authorities and to data subjects; and being audited periodically.

The security rules under the Standard, while not mandatory or subject to penalties, suggest that controllers (translated in Shi et. al, 2019, Sec.10):

- Grant the data subjects' access to their personal information and authorize modification, copying, and downloading,
- Maintain data processing records,
- Appoint a Chief Information Security Officer,
- Carry out staff training regarding personal data processing at least once a year,
- Conduct security testing prior to releasing products or services,
- Have a dedicated information security team if processing information about more than 500,000 persons.

The data protection framework in China addresses national security risk, widening its reach in comparison to the GDPR. Although both the Standard and the GDPR address impact assessments, the Standard is more specific about the suggested frequency and notes that the assessment reports should be made "accessible in an appropriate manner" (translated in Shi et. al, 2019, Sec. 10(2)(e)). Note that the Standard is not binding on firms while the GDPR is binding. Also, the Standard sets no severity threshold or duration for reporting cybersecurity incidents to data subjects and third parties processing personal data are subject to security assessments. The Standard also suggests notification if a processor is "unable to offer an adequate level of security." Local practitioners see the Standard's provisions as indicative of possible future directions by Chinese legislators.

United States

At the federal level, individuals and companies doing business in the United States are required to implement adequate measures for the protection of sensitive personal data (DLA Piper, 2019c). The FTC has determined that a lack of reasonable data security measures is an "unfair practice". Additionally, the FTC's behavioral advertising principles recommend reasonable data security measures about consumer data for behavioral advertising (DLA Piper, 2019c).

Entities subject to HIPAA or financial services regulations are subject to stricter security requirements. Some states require additional data security measures (DLA Piper, 2019c). For example, data controllers in Massachusetts and Nevada must use encryption when storing and transferring sensitive personal data. The United States is notable for developing breach notification requirements, which are currently enforced by all of its states and most of its territories (DLA Piper, 2019c, p.5). Most state data breach laws require entities to implement reasonable security measures to protect the personal data covered by those laws.

India

The IT Rules provide that any "body corporate" which handles sensitive personal data must implement "reasonable security practices and procedures" regarding sensitive personal data that are commensurate with the information assets being protected (IT Rules, 2011, Rule 4(v)). These can be agreed upon by the parties, or in the absence of such agreement, the IT Rules suggest using the International Standard Requirements or a code established by a trade association and approved by the central government (IT Rules, 2011, Rule 8(2)). The IS/ISO/IECD 270001 standards are provided as an example. In the event of a breach, the body corporate may be called upon to show that these standards have been adhered to. There are penalties specified for failure to secure sensitive data.

Like the GDPR, the *Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules* of 2013 require that data controllers inform the Cert-in (a response agency notified by the Government) of specific kinds of data security breach.

Colombia

In Colombia, *Law 1266* provides that data processors must implement security systems with technical safeguards to ensure the safety and accuracy of the data, and to prevent damage, loss and unauthorized use of or access to the data. Similarly*, Law 1581* and *Decree 1074 of 2015* require that data protection processors and controllers implement the necessary technical, physical and administrative safeguards to ensure the safety of databases and to prevent their damage, loss and unauthorized use or access (DLA Piper, 2019a). However, unlike China's tiered system, Colombia only requires data controllers and processors to make a good faith effort towards security and currently lacks explicit recommendations on how to actually carry this out.

United Arab Emirates

Although there are no general guidelines regarding data security, sectoral laws do provide some rules. The *Telecommunications Law*, passed by Decree no. 3 of 2003, addresses the collection of data through any means of telecommunications, including through service providers (DLA Piper, 2019b). The Telecoms Regulatory Authority (hereinafter "TRA") was established by the *Telecommunications Law* to represent consumer interests and oversee the telecommunications sector in the UAE as a whole. *TRA Consumer Protection Regulations Version 3.1 of 2017* aims to protect the information of telecommunication subscribers. Subscriber information is defined as any personal data including but not limited to:

- Name and address,
- Bank account and credit card details,
- Records of calls or messages,
- Service usage details,
- Account status,
- Payment history and credit rating.

The regulations require licensees to take "all reasonable measures" to protect the privacy of subscribers (DLA Piper, 2019b). The TRA Consumer Protection Regulations provide that licensees must obtain a subscriber's prior consent before sharing any subscriber information with their affiliates and/or other third parties. However, the form and content of consent are not specified.

In the DIFC, secure IT infrastructures and appropriate organizational measures are required when storing and retaining personal data (Bowden and Kasuya, 2017). Dubai Law No. 28 of 2015 restricts the disclosure of personal data obtained through a census, poll or study by the Dubai Statistics Centre. The DIFC imposes data breach notification requirements on data controllers (Bowden and Kasuya, 2017).

What principles exist for data processors?

European Union

Article 8 of the *EU Charter of Fundamental Rights* states,

> Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified (Charter of Fundamental Rights of the EU, 2012, Art.8).

The following are the seven key principles related to the processing of personal data, as provided in Article 5 of the GDPR:

1) **Lawfulness, fairness and transparency:** Valid grounds for collecting and using personal data should be identified, and not in a way that is unduly detrimental, unexpected or misleading to the individuals concerned. Organizations should be clear, open and honest about how the personal data will be used.

2) **Purpose limitation:** Personal data should be collected for a specified, explicit and legitimate purpose and not for an incompatible purpose, unless archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes.

3) **Data minimization:** Data collection should be adequate, relevant and limited to what is necessary.

4) **Accuracy:** Data should be accurate and up to date. Depending on the purpose of the data, inaccuracies should be erased or rectified without delay.

5) **Storage limitation:** Data should be kept in a form that permits identification for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for a longer period for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to the implementation of the appropriate technical and organizational measures to safeguard the rights and freedoms of the individuals.

6) **Integrity and confidentiality:** The security of the personal data must be ensured, including protecting it from unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

7) **Accountability:** Organizations should be responsible for and able to demonstrate compliance with the above six principles.

Several guidelines and checklists have been published to help data controllers fulfil each principle, such as from the Information Commissioner's Office in the United Kingdom (Information Commissioner's Office, n.d.)

China

The Personal Information Provisions provide general principles that telecommunication and internet service providers shall collect and use personal data in a lawful and proper manner and by following the principle of necessity (translated in Creemers, 2013).

The Standard provides principles including transparency, specificity, purpose, and security. It introduces data subject rights, including the rights of erasure and data portability (translated in Shi et. al, 2019).

1) **Transparency**: Data subjects should be informed regarding data collection, according to the type of information and the manner of collecting it.

2) **Specificity**: Personal data collected must be directly related to the services provided by the entity.

3) **Purpose**: Use of personal data should be reasonably linked with the original purpose of collection.

4) **Security**: Data controllers must implement data security measures, including appointing key personnel responsible for data security and conducting periodic impact assessments.

United States

Although there is no national law providing a set of data protection principles in the United States, the laws and regulations discussed in Section 1 of this analysis provide some overarching guidance and requirements with respect to the personal data protected thereby. Both GLBA and HIPAA, for example, contain requirements for notice and data security. In addition, the FTC provides Self-Regulatory Principles for Online Behavioral Advertising (FTC, 2009):

1) **Transparency and consumer control:** Websites should inform consumers about their data collection practices and give consumers the option to opt-put.

2) **Reasonable security, and limited data retention for consumer data**: Companies should implement reasonable measures for data security, according to the company's circumstances and the nature of the data. Data should not be retained longer than necessary to meet a legitimate business or law enforcement need.

3) **Affirmative express consent for material changes to existing privacy promises:** Companies should obtain express consent from consumers when using previously collected data in a manner that is materially different than that expressed in its original privacy policy.

4) **Affirmative express consent to (or prohibition against) using sensitive data for behavioral advertising:** express consent should be obtained from consumers before companies can collect sensitive personal data for behavioral advertising.

India

Although limited, the IT Rules contain several principles for data processing (IT Rules, 2011):

1) **Lawfulness**: Sensitive personal data may only be collected for a lawful purpose.

2) **Transparency:** Body corporates dealing with sensitive personal data must publish their privacy policy on their website, containing the nature and purpose of usage of information, including their security practices. Data controllers must also appoint a Grievance Officer and publish their contact information on their website.

3) **Purpose limitation**: Sensitive personal data may only be used for the purpose for which it was originally collected.

4) **Collection limitation**: Sensitive personal data may only be collected for a lawful purpose connected with a function or activity of the body corporate and such collection is necessary for that purpose.

5) **Security:** Body corporates must implement adequate security practices for sensitive personal data.

6) **User rights**: The IT rules provide users with certain rights that must be provided by the body corporates:

    - **Right of review and correction:** Providers of personal data and sensitive personal data must be permitted to review the information provided by them, and correct or amend any inaccurate or deficient information.
    - **Right to deny and withdraw consent:** Providers of information, including sensitive personal data, must be given the option to not provide the information sought. They must also have the option to withdraw previously given consent at any time by writing to the body corporate.
    - **Right of grievance redressal:** Providers of information must be able to seek redress of their grievances. The IT Rules mandate the appointment of a Grievance Officer for this purpose, who must redress the grievances within one month of their receipt.

The principles of data processors would significantly change under the PDP Bill, which prescribes strict data protection obligations (fair and reasonable processing, purpose limitation, collection limitation, etc.), specific grounds for processing of data, and institutes a regulator with the power to specify data protection standards and conduct audits in certain cases (PDP Bill, 2018).

Colombia

Colombia's data protection law lists a comprehensive set of principles regarding data processing (Adarve and Acosta, 2017; DLA Piper, 2019a):

1) **Lawfulness**: Applies to processing of a regulated activity that must subject to the Law.

2) **Purpose**: Processing must follow a legitimate purpose according to the Constitution and the Law, which would be disclosed to the data subject.

3) **Freedom**: Processing may only be carried out under the prior, express, and informed consent of the data subject. Personal data may not be obtained or disclosed without prior authorization or without a legal or judicial mandate which replaces consent.

4) **Accuracy or quality**: Information subject to processing must be truthful, complete, exact, updated, verifiable, and comprehensible. Processing is prohibited for partial, incomplete, fractioned, or error inducing data.

5) **Transparency**: Processing must guarantee the data subject's right to obtain at any time and without restrictions, information about the existence of data that concerns the data subject.

6) **Access and restricted circulation**: Processing is subject to the limits that flow from the nature of the personal data, the provisions of this law and the Constitution. In that sense, processing may only be carried out by persons authorized by the data subject and/or persons provided by the law. Personal data, except for public information, may not be available online or in any other means of disclosure, unless the access is technically controllable to offer a restricted access only to data subject or authorized third parties according to this law.

7) **Security**: Data subject to processing must be managed with technical, human, and administrative measures that are necessary to grant security to the registry avoiding their unauthorized alteration, loss, access, use, consultation.

8) **Confidentiality**: All persons that intervene with the processing of personal data that are not of public nature must guarantee the preservation of the information, including after the relationship with any of the acts under processing are finalized. Supply and communication of the personal data is only possible when it applies to the development of the authorized activities under this law.

United Arab Emirates

As discussed above, the UAE as a whole does not have a specific data protection law. In the ADGM and the DIFC, data controllers are required to ensure that the personal data that they process are (DFIC Data Protection Law, 2018, Art.8):

1) Processed fairly, lawfully and securely,

2) Processed for specified, explicit and legitimate purposes in accordance with the data subject's rights,

3) Adequate, relevant and not excessive in relation to the purposes for which they are collected or further processed,

4) Accurate and, where necessary, kept up to date,

5) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data were collected or for which they are further processed.

How are these principles enforced and what are the penalties for violators?

European Union

Under the GDPR, each Member State's must appoint a National Data Protection Authority (hereinafter "DPA") who is responsible for implementing and enforcing data protection law in its jurisdiction (Gabel and Hickman, 2019a). Member States must establish their own rules on penalties, including criminal penalties for violations of GDPR not covered by the Regulation or for infringement of domestic legislation (Gabel and Hickman, 2019b; GDPR, 2016, Art. 84). National authorities may issue administrative fines for violations, as well as orders for compliance and even bans on data processing (Gabel and Hickman, 2019b; GDPR, 2016, Art. 83). The fines imposed under GDPR are significant. Depending on the violation, fines can reach €20 million or four percent of the total worldwide annual turnover of the previous financial year (Gabel and Hickman, 2019).

The majority of EU Member States have adopted national laws to comply with the GDPR (European Commission, 2019).[7] As of September, around eighty two fines and penalties have been issued by DPAs under the GDPR—with fines ranging from €118 to €204 million (GDPR Enforcement Tracker, n.d).[8] In January 2019, the French DPA, the CNIL, issued the first major GDPR decision, fining Google €50 million for failing to comply with the Regulation's transparency provisions (Romm, 2019a). The CNIL had received complaints from privacy activists prior to the enactment of the GDPR, and as soon as the Regulation came into force, official investigations were launched into the tech giant's practices. Although Google had made adjustments to comply with the GDPR, the French regulator found that the company was not clear about the way it was collecting its users' data (Romm, 2019a).

China

China has no single authority responsible for enforcing privacy protections. Under its Cybersecurity Law (hereinafter "CSL"), the Cyberspace Administration of China (CAC) is responsible for the planning and coordination of cybersecurity and relevant supervisory and administrative work, while the Ministry of Industry and Information Technology, the public security department, and other relevant departments are responsible for the supervision and administration of personal information protection in their respective sectors. The State Administration for Industry and Commerce and its local counterparts are responsible for the supervision and administration of personal information of consumers.

The CSL allows for fines and modification orders in the case of violations. Violators are subject to fines up to RMB 1,000,000 (almost 150,000 USD) or actions such as suspending operations, taking down websites or losing business permits. Additionally, individuals may claim protections under Tort Liability Law as well as the Criminal Law, under which violators are subject to compliance orders, monetary fines, and imprisonment.

United States

The United States has no one national authority responsible for data protection (DLA Piper, 2019c). Under the Federal Trade Commission (hereinafter "FTC") Act, the FTC has assumed the power to

[7] As of July 2019, all but three Member States— Greece, Portugal and Slovenia—have updated their national data protection laws in line with EU rules.

[8] In July 2019, the Information Commissioner (ICO) in the United Kingdom issued a notice of its intention to fine British Airways £183.39M for GDPR infringements which likely involve a breach of Art. 32 GDPR stemming from a cyber incident in September 2018.

broadly enforce privacy regulation in the consumer context and specifically regulates certain regulations relating to email and children's online privacy (DLA Piper, 2019c). Additionally, State Attorneys have enforcement powers, and sector-specific regulators are responsible for issuing and enforcing regulations in areas such as healthcare and financial services. Data privacy as a preventative obligation is not heavily regulated outside these fields. The FTC is the federal agency that most broadly regulates the privacy practices of companies with respect to consumers.

Although the United States is more flexible than other countries in terms of data protection regulations, violators of the existing rules are subject to penalties. The FTC has brought enforcement actions against companies such as Facebook, Google and Microsoft regarding the collection, use and processing of personal data. If the FTC suspects that a company's privacy or data security practices are unfair or deceptive, the agency can initiate an investigation. Violations can result in fines, injunctions, and imprisonment (Jolly, 2018). Settlements sometimes include reporting requirements, as well as third-party audits and monitoring.

Since the Cambridge Analytica scandal in 2018, the FTC has been investigating Facebook for the company's mishandling of its users' personal data. In 2011, the FTC had ordered Facebook improve its data policies, and if it is found to have broken that agreement, the company would be subject to a multi-billion dollar fine (Romm, 2019b). This would surpass the highest fine imposed by the FTC to date.[9] in 2012, the FTC ordered Google to pay 22.5 million USD for breaching a prior settlement where the tech giant had agreed to be clear about the extent to which its users could exercise control over the collection of their data (Romm, 2019b). Under the California Consumer Privacy Act, each individual who is victim of a data breach that results from the lack of reasonable data security measures may claim up to 750 USD, placing non-compliant businesses at great risks for class action lawsuits (DLA Piper, 2019c).

In addition, various state and federal regulators enforce compliance with GLB. The Office of Civil Rights within the Department of Health and Human Services enforces HIPAA and has issued notable fines against covered entities that have failed to adequately protect HPI from unauthorized disclosure.

Many U.S. companies participate in self-regulatory programs to promulgate their codes of conduct, often oriented to best business practices (e.g., the Digital Advertising Alliance (DAA) for online behavioral advertising, and the Children's Advertising Review Unit (CARU) for companies advertising to children).

Section 230 of the *Communications Decency Act* of 1996 stipulates that online platforms, unlike their analog counterparts, are not liable for the content posted by their users. By exempting Facebook, Google, Twitter and others from stifling legal and regulatory risks, the provision powered the rapid growth of the U.S. technology industry. But it also absolved those companies of any blame regarding what third parties were doing with users' data.

India

There is currently no national regulator for data protection in India. Claims for such compensation must be brought to the Adjudicating Officer appointed by the Indian Government under the IT Act or the competent civil court, depending on the amount of injury or damage (IT Act, 2008, Art. 46). The IT Act

[9] Editor's Note: On July 24, 2019, the FTC imposed a $5 billion fine on Facebook, which imposed sweeping new privacy restrictions on the company alongside the penalty. See: FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook: https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions. Many privacy and consumer advocates have been frustrated with the size of the settlement, arguing that it could have been even higher and pointing to the jump in Facebook's share price as evidence of markets reacting positively to news of the penalty's size.

provides for compensation as well as penalties for certain violations related to data protection (IT Act, 2008, Art. 43).

When a body corporate is negligent in implementing and maintaining reasonable security practices, it is liable to pay uncapped compensation to the person affected. Other contraventions may give rise to compensation or penalty up to INR 25,000 (approx. USD 365) to the person affected. Further, any person who discloses any personal information about another person with the intention or knowledge to cause wrongful gain or loss, is liable to imprisonment for up to 3 years and/or fines up to INR 500,000 (approx. USD 7,300).

The penalties are significantly higher under the PDP Bill, and a broader range of offenses are specified in it. The PDP Bill envisages the establishment of a Data Protection Authority, who will prescribe security standards for different types of data. Failure to adhere to such standards would result in heavy penalties that may extend up to INR 150,000,000 (approx. USD 2,190, 787.15) or four percent of its total worldwide turnover of the preceding financial year, whichever is higher (PDP Bill, 2018, Art.69).

Colombia

The Superintendence of Industry and Commerce (hereinafter “SIC”) serves as the primary data protection authority to resolve claims related to data protection, noncompliance investigations and the imposition of sanctions. However, the Financial Superintendence may step in if the personal data involves financial and credit-reporting laws, and any party relating to the data processing is an entity under its supervision. Additionally, the General Controller’s Office investigates noncompliance and data breaches involving public authorities.

Colombian citizens may seek redress via constitutional action for mishandling of their personal data (DLA Piper, 2019a). A judicial order can compel the modification, security, or erasure of personal, and the lack of compliance with such order is punishable by imprisonment. Additionally, under the Criminal Code, whoever obtains, compiles, subtracts, offers, sells, exchanges, sends, buys, intercepts, discloses, modifies, or employs personal codes and personal data contained in files, databases or similar means, without the capacity to do so, can be subject to up to eight years of prison time and up to 200,000 USD in fines. The SIC may also impose fines up to 400,000 USD or foreclose a private entity it finds to be in violation (DLA Piper, 2019a).

When it comes to data privacy and protection, observers report the SIC has focused mainly on seeking compliance rather than on imposing penalties. The agency aims to help companies comply with the laws, organizing events with stakeholders to offer guidance. In recent months the agency has expanded in terms of human resources, which may indicate its desire to bolster its supervisory duties (Alcazar, 2018). Most recently, it ordered Facebook strengthen its data security measures, after discovering that the Cambridge Analytica scandal had affected seventy-four Colombian citizens (Cifuentes, 2019). The social media company must engage a private auditor and periodically report its improvements to the SIC. According to *Resolution 1321 of January 24, 2019*, the measures must be **“**appropriate, useful, efficient, and provable to fully comply with Colombian data protection laws” (Cifuentes, 2019). Facebook has four months to comply, otherwise it could be subject to monetary fines.

While supportive of the general approach of the law, practitioners question its scope and ambition, particularly when considering the resources required by data controllers in the country to comply with the law’s requirements.

United Arab Emirates

The UAE has no national authority responsible of data protection (Dowle, 2018). Different agencies, such as the TRA and the Central Bank, regulate specific sectors in this regard. Additionally, each Emirate has a cybercrime unit that deals with breaches of the Federal Cybercrime Law (DLA Piper, 2019b). Depending on the nature of the crime, violators are subject to fines up to AED 1,000,000 (about 275,000 USD) and imprisonment (DLA Piper, 2019b).

The ADGM has its own regulating body, the Office of Data Protection. It may issue directions, warnings, and recommendations for compliance. Data controllers who fail to comply with a direction or any rules under the DPR 2015 are subject to fines. In the DIFC, the Commissioner of Data Protection (CDP) is responsible for carrying out investigations and issuing notices and compliance orders to violators. Failure to comply with an order from the CDP may result in a fine or a court order.

Local practitioners report they are unaware of, and could not find after investigation, examples of fines or other punishments against firms under the DIFC or ADGM data protection regulations.

Annex 1: Recent and ongoing reforms elsewhere around the world

Following the increased attention to data privacy rights and obligations due to the development and enactment of the GDPR in May 2018, countries around the world have sought to update their national laws and regulations to keep up with the global data privacy climate. While not analyzed in depth in the above paper, several of those country updates are highlighted below.

Brazil	**In August 2018, Brazil approved the "General Data Protection Law", applying to data processing in Brazil as well as any activities outside that affect Brazilian domiciled data subjects (Law No. 13.709 of 14 August 2018, 2018). The law includes provisions on the collection and handling of personal data by public and private entities. Prior consent is required for data processing although the law has more legal bases to process data than the GDPR. Additionally, it grants data subjects rights to access, correct, and erase their data. The "adequacy approach" is adopted with regard to cross-border data transfers. Finally, non-compliant data processors are subject to fines.**
Japan	Japan was the first country within the Asia-Pacific Economy Cooperation (APEC) to be recognized by the EU to have "adequate levels of data protection". Following the introduction of GDPR, Japan and the EU finalized an agreement allowing the free flow of data between the two parties (Focal Point Insights, 2018).
Mexico	Mexico announced in June 2018 that it was adopting the Council of Europe Convention 108 for the "Protection of Individuals with regard to Automatic Processing of Personal Data" as well as its "Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and cross border data flows".
New Zealand	New Zealand introduced a new privacy bill in March 2018 which, if approved, would replace the Privacy Act 1993 (Justice Committee New Zealand, 2018). The bill includes provisions for data subject's privacy with regard to the collection, storage, and use of their personal data, while including bases for legitimate use of the data. It grants the Privacy Commissioner stronger powers, such as the ability to make binding decisions on data access requests and to issue compliance notices to data processors.
Singapore	In 2017, the PDPC held public the first public consultations reviewing the Personal Data Protection Act 2012 (Personal Data Protection Commission Singapore, n.d.). Topics for review included alternatives to consent for the collection, use, and disclosure of personal data, as well as new mandatory regime for data breach notifications. Public consultations were held again in 2018 on "Managing Unsolicited Commercial Messages and the Provision of Guidance to support Innovation in the Digital Economy". Proposed reform included an "Enhanced Practical Guidance" framework which would give the PDPC the power to assist organizations with regulatory compliance, as well as exceptions on the collection, use, or disclosure of personal data without the data subject's consent.

Annex 2: Key definitions surrounding data privacy and security

The table below contains key definitions and terms that are found in the various regulations analyzed in this paper:[10]

Anonymization	**EU: The processing of personal data in such a manner that the data subject is not or no longer identifiable.** ***Anonymized data is not subject to the GDPR.** **China: Through the technical processing of personal information, the personal information subject cannot be identified, and the processed information cannot be processed. Note: the information obtained after anonymization of personal information is not personal information.**
Controller	**EU**: The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. **China**: Any private or public organization that has the right to determine the purpose and manner of processing personal information. **Colombia**: Natural or legal person, public or private, who alone or with others, makes decisions over the data set and/or the data processing. **UAE:** ADGM: Any person in the Abu Dhabi Global Market (excluding a natural person acting in his capacity as a staff member) who alone or jointly with others determines the purposes and means of the processing of personal data.
Personal Data	**EU**: Any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, *directly or indirectly*, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. **China**: Information that identifies a natural person either by itself or in combination with other information. This includes information that will reflect the activities of an identified natural persons. **Colombia**: Any information linked or which could be linked to one or more identified or identifiable natural persons. **India**: Any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person. **UAE:** ADGM: Any information relating to an identified natural person or identifiable natural person.

[10] Definitions vary widely by regulation, sector, and type of statute in the United States. As such, they are not included here.

	DIFC: Any data referring to an Identifiable Natural Person (a natural living person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his biological, physical, biometric, physiological, mental, economic, cultural or social identity).
Processing	**EU:** Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. **Colombia**: Any operation or set of operations on personal data, such as collection, storage, use, dissemination, or destruction. **UAE:** ADGM: Any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. DIFC: Any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
Processor	**EU**: A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. **Colombia**: A natural or legal person, public or private, which, on its own or with others, processes the data set on behalf of the controller. **UAE:** ADGM: Any person (excluding a natural person acting in his capacity as a staff member) who processes personal data on behalf of a data controller. DIFC: Any data referring to an Identifiable Natural Person.
Pseudonymization	**EU**: The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. **China**: De-identification through the technical processing of personal information, it is impossible to identify personal information without additional information. Note: De-identification is based on individual, retaining individual granularity, using pseudo-name, encryption, hash function and other technical means. Replace the identification of personal information.

Personal Data Breach	**EU:** A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Sensitive Data	**EU:** Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. **China**: Information which, if leaked, illegally provided or used without authorization, will endanger human rights and property security, easily lead to damage to reputation, physical and mental health or discriminatory treatment. **Colombia:** Data that relates to the intimacy of the data owner, or that, if disclosed without consent, could lead to discrimination, such as data revealing racial or ethnic origin, political orientation, religious or philosophical beliefs, trade-union membership, social organizations, human rights organizations, or those organizations that promote the interests of any political party or that ensure the rights and guarantees of opposition political parties, as well as data relating to health, sexual life and biometrics. **India:** Such personal information which consists of information relating to password; financial information such as bank account or credit card or debit card or other payment instrument details; physical, physiological and mental health condition; sexual orientation; medical records and history; biometric information; any detail relating to the above clauses as provided to body corporate for providing service; and any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise: provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules. **UAE:** ADGM: Personal data revealing or concerning (directly or indirectly) racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and health or sex life. DIFC: Personal data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership and health or sex life.

Annex 3: Resources for worldwide data protection and privacy updates

The table below highlights a few helpful, free databases and resources for readers to keep up to date on the latest data protection and privacy developments around the world.

Title	Description	Link
DLA Piper – Data Protection Laws of the World	This handbook sets out an overview of the key privacy and data protection laws and regulations across nearly 100 different jurisdictions and offers a primer to businesses as they consider this complex and increasingly important area of compliance. Download individual country reports, compare countries, or download the whole handbook.	https://www.dlapiperdataprotection.com/
The International Comparative Legal Guides (ICLG) to Data Protection Laws and Regulations 2019	The ICLG to Data Protection Laws and Regulations covers relevant legislation and competent authorities, territorial scope, key principles, individual rights, registration, formalities, appointment of data protection officer and of processors – in 42 jurisdictions.	https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa
UNCTAD Cyberlaw Tracker: Data Protection and Privacy Legislation Worldwide	The UNCTAD Global Cyberlaw Tracker is the first ever global mapping of cyberlaws. It tracks the state of e-commerce legislation in the field of e-transactions, consumer protection, data protection/privacy and cybercrime adoption in the 194 UNCTAD member states.	https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx

References

The Aadhaar and Other Laws (Amendment) Act, 2019 (2019, July 23). Retrieved from https://uidai.gov.in/images/news/Amendment_Act_2019.pdf

Adarve, L. H., and Acosta, J. (2017). *Data Protection: Colombia.* Retrieved from https://dentons.cardenas-cardenas.com/en/insights/articles/2017/july/28/-/media/e968e3912aed44358393bd7cb32b0d56.ashx

Alcázar, H.F. (2018, November 17) Changes are coming in the Superintendence of Industry and Commerce. *El Universal*. Retrieved from https://www.eluniversal.com.co/economica/se-avecinan-cambios-en-la-superintendencia-de-industria-y-comercio-292069-LVEU410128

Article 29 Working Party (2014, April). *Opinion 05/2014 on Anonymisation Techniques.* Retrieved from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

Bowden, J. and Kasuya, K. (2017) *United Arab Emirates*. Retrieved from https://interactiveguides.lexmundi.com/lexmundi/global-data-privacy/united-arab-emirates

Chabinsky, S. and F.P. Pittman (2019). USA: Data Protection 2019. In Gabel, D. and Hickman T. (Eds.), *The International Comparative Legal Guides to Data Protection Laws and Regulations 2019.* London: Global Legal Group. Retrieved from https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa

Charter of Fundamental Rights of the European Union (2012) Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

Cifuentes, V. (2019, January 28) SIC asks Facebook for more security measures after incident with 74 profiles. *La Republica.* Retrieved from https://www.larepublica.co/empresas/sic-pide-a-facebook-mayores-medidas-de-seguridad-tras-incidente-con-74-perfiles-2821202

Coos, A. (2019, June 21). *India's Personal Data Protection Bill: What We Know so Far.* [Blog post]. Retrieved from https://www.endpointprotector.com/blog/indias-personal-data-protection-bill-what-we-know-so-far/

Creemers, R. (2013, July 16) Telecommunications and Internet Personal User Data Protection Regulations. [Blog post]. Retrieved from https://chinacopyrightandmedia.wordpress.com/2013/07/16/telecommunications-and-internet-user-individual-information-protection-regulations/

Creemers, R., Trilolo, P., and Webster, G. (2018) *Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017).* Retrieved from https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/

Deloitte (2019) *India Draft Personal Data Protection Bill, 2018 and EU General Data Protection*

Regulation: A comparative view. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-india-draft-personal-data-protection-bill-noexp.pdf

DIFC Data Protection Law No. 1 of 2007. (2018, January) Retrieved from https://www.difc.ae/files/3615/1739/8803/Data_Protection_Law_DIFC_Law_No._1_of_2007.pdf

DLA Piper (2019a). *Data Protection Laws of the World: Colombia*. Retrieved from https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country-1=CO

DLA Piper (2019b). *Data Protection Laws of the World: United Arab Emirates*. Retrieved from https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country-1=AE

DLA Piper (2019c). *Data Protection Laws of the World: United States*. Retrieved from https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country-1=US

Dowle, C. (2018). *Data protection in United Arab Emirates: overview*. Retrieved from https://uk.practicallaw.thomsonreuters.com/0-518-8836?transitionType=Default&contextData=%28sc.Default%29

European Commission (2019, July 24) *General Data Protection Regulation shows results, but work needs to continue*. [Press Release].Retrieved from https://europa.eu/rapid/press-release_IP-19-4449_en.htm

European Data Protection Board (2019). *First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities.* Retrieved from https://edpb.europa.eu/sites/edpb/files/files/file1/19_2019_edpb_written_report_to_libe_en.pdf

Farrell, H. (2019, April 4). Facebook is finally learning to love privacy laws. *The Financial Times*. Retrieved from https://www.ft.com/content/67b25894-5621-11e9-8b71-f5b0066105fe

Federal Communications Commission (2016). Protecting the Privacy of Customers of Broadband and Other Telecommunications Services. *Federal Register*, 81(232) Retrieved from https://www.govinfo.gov/content/pkg/FR-2016-12-02/pdf/2016-28006.pdf

Federal Trade Commission (2009, February*) FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising: Tracking, Targeting, & Technology.* Retrieved from https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf

Focal Point Insights (2018, July 26) Why the EU-Japan Data Transfer Agreement Is So Significant. *[Blog post]* Retrieved from https://blog.focal-point.com/why-the-eu-japan-data-transfer-agreement-is-so-significant

Gabel, D. and Hickman, T. (2019a) Chapter 14: Data Protection Authorities. In *Unlocking the*

EU General Data Protection Regulation: A practical handbook on the EU's new data protection law. White & Case. Retrieved from https://www.whitecase.com/publications/article/chapter-14-data-protection-authorities-unlocking-eu-general-data-protection

Gabel, D. and Hickman, T. (2019b) Chapter 16: Remedies and sanctions. In *Unlocking the EU General Data Protection Regulation: A practical handbook on the EU's new data protection law*. White & Case. Retrieved from https://www.whitecase.com/publications/article/chapter-16-remedies-and-sanctions-unlocking-eu-general-data-protection#toc

Government of Colombia (2018). *The Superintendency of Industry and Commerce.* Retrieved from http://www.camara.gov.co/sites/default/files/2018-09/Respuesta%20Superintendencia%20de%20Industria%20y%20Comercio.pdf

Greenleaf, G. (2018). *Global Convergence of Data Privacy Standards and Laws: Speaking Notes for the European Commission Events on the Launch of the General Data Protection Regulation (GDPR) in Brussels & New Delhi, 25 May 2018.* UNSW Law Research Paper No. 18-56. Retrieved from https://ssrn.com/abstract=3184548

Global Media Insight (2019, September 1) United Arab Emirates Population Statistics (2019). [Blog post] Retrieved from https://www.globalmediainsight.com/blog/uae-population-statistics/

IAPP-EY. (2018). *Annual Privacy Governance Report*. Retrieved from https://iapp.org/media/pdf/resource_center/IAPP-EY-Gov_Report_2018-FINAL.pdf.

Information Commissioner's Office (n.d.). *The Principles*. Retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

Information Commissioner's Office (2012). *Anonymisation: managing data protection risk code of practice*. Retrieved from https://ico.org.uk/media/1061/anonymisation-code.pdf

Information Commissioner's Office (2019). *Intention to fine British Airways £183.39m under GDPR for data breach.* [Official Statement]. Retrieved from https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/

Information Technology Rules, 2011 (2011). Retrieved from https://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf

Information Technology Act, 2008 (2008). Retrieved from http://nagapol.gov.in/PDF/IT%20Act%20(Amendments)2008.pdf

Jolly, L. (2018). *Data protection in the United States: overview*. Retrieved from https://uk.practicallaw.thomsonreuters.com/Document/I02064fbd1cb611e38578f7ccc38dcbee/View/FullText.html

Justice Committee New Zealand (2018) *Privacy Bill Commentary: Government Bill 34-2 as reported from the Justice Committee.* Retrieved from http://www.legislation.govt.nz/bill/government/2018/0034/latest/096be8ed8184b90a.pdf

Justice K.S. Puttaswamy (Retd) vs Union Of India (2018). Case No. Writ petition (Civil) No. 494 of 2012. Retrieved from https://sci.gov.in/pdf/LU/ALL%20WP(C)%20No.494%20of%202012%20Right%20to%20Privacy.pdf

Law No. 13.709 of 14 August 2018 (2018). Retrieved from http://www.normaslegais.com.br/legislacao/lei-13709-2018.htm

Ning, S. and H. Wu (2019). China: Data Protection 2019. In Gabel, D. and Hickman T. (Eds.), *The International Comparative Legal Guides to Data Protection Laws and Regulations 2019.* London: Global Legal Group. Retrieved from https://iclg.com/practice-areas/data-protection-laws-and-regulations/china.

Personal Data Protection Bill, 2018 (2018). Retrieved from https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

Personal Data Protection Commission Singapore (n.d.) *Public Consultations. Jul-Sep 2017: Public Consultation on Approaches to Managing Personal Data in the Digital Economy.* Retrieved from https://www.pdpc.gov.sg/Legislation-and-Guidelines/Public-Consultations#ACTR1

Personal Data Protection Commission Singapore (2018, January). *Guide to Basic Data Anonymisation Techniques*. Retrieved from https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf

Public Law 115–22 (2017, April 3). Retrieved from https://www.congress.gov/115/plaws/publ22/PLAW-115publ22.pdf

Regulation (EU) 2016/679 General Data Protection Regulation (2016, April 27). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679

Responsible Data. (n.d.). *What is Responsible Data?* Retrieved from https://responsibledata.io/.

Romm, T. (2019a, January 21). France fines Google nearly $57 million for first major violation of new European privacy regime. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/europe/france-fines-google-nearly-57-million-for-first-major-violation-of-new-european-privacy-regime/2019/01/21/89e7ee08-1d8f-11e9-a759-2b8541bbbe20_story.html?utm_term=.ee8c355f84a0

Romm, T. (2019b, February 14). The U.S. government and Facebook are negotiating a record, multibillion-dollar fine for the company's privacy lapses. *The Washington Post*. Retrieved from https://www.washingtonpost.com/technology/2019/02/14/us-government-facebook-are-negotiating-record-multi-billion-dollar-fine-companys-privacylapses/?noredirect=on&utm_term=.c428636b6d67

Sacks, S. (2018) *Critical Questions: New China Data Privacy Standard Looks More Far-Reaching than GDPR.* Retrieved from https://www.csis.org/analysis/new-china-data-privacy-standard-looks-more-far-reaching-gdpr

Senate Bill 5376 Protecting Consumer Data (2019, March 6). Retrieved from http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bill%20Reports/Senate/5376-S2%20SBR%20APS%2019.pdf

Shi, M., Sacks, S., Chen, Q., and Webster, G. (2019, February 8) Translation: China's Personal Information Security Specification: The Chinese government's first major digital privacy rules. [Blog post] Retrieved from https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-personal-information-security-specification/#targetText=The%20Personal%20Information%20Security%20Specification%20took%20effect%20in%20May%202018.&targetText=While%20the%202017%20Cybersecurity%20Law,emerging%20system%20around%20personal%20data.

Solon, O. (2018, October 3). Facebook faces $1.6bn fine and formal investigation over massive data breach. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2018/oct/03/facebook-data-breach-latest-fine-investigation

Subramaniam, H., Subramaniam, A. (2019). India: Data Protection 2019. In Gabel, D. and Hickman T. (Eds.), *The International Comparative Legal Guides to Data Protection Laws and Regulations 2019.* London: Global Legal Group. Retrieved from https://iclg.com/practice-areas/data-protection-laws-and-regulations/india

Temple-Raston, D. (2018, October 8). Why the Tech Industry Wants Federal Control Over Data Privacy Laws. *NPR.* Retrieved from https://www.npr.org/2018/10/08/654893289/why-the-tech-industry-wants-federal-control-over-data-privacy-laws

United Arab Emirates's Constitution of 1971 with Amendments through 2004 (2004). Retrieved from https://www.constituteproject.org/constitution/United_Arab_Emirates_2004.pdf

United Nations Conference on Trade and Development. (2019). *Data Protection and Privacy Legislation Worldwide*. Retrieved from https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx.

Wilmap (2017) *Justice K.S. Puttaswamy (Retd) & Anr v. Union of India & Ors*. Retrieved from https://wilmap.law.stanford.edu/entries/justice-ksputtaswamyretd-anr-v-union-india-ors