2020 Wolters Kluwer China
Law & Reference Compliance Guide Series

Globalization and Privacy Protection Guide

环球律师事务所 GLOBAL LAW OFFICE SINCE 1979

Wolters Kluwer | 威科先行®

环球律师事务所
GLOBAL LAW OFFICE
SINCE 1979
环球律师事务所
GLOBAL LAW OFFICE
SINCE 1979

Foreword

Basing on the needs of China's legal service market and Wolters Kluwer's 180 years of professional service experience, we present 2020 Wolters Kluwer China Law & Reference Compliance Guide Series to China's legal professionals. Authors of the series are experienced and outstanding teams of lawyer from various practice firlds. The 2020 Wolters Kluwer China Law & Reference Compliance Guide Series include four spotlight topics of Cyber Security, Finance, Anti-Bribery and Labor Law. With ideas drawn from multi-dimensional views, we aim to provide practical legal guidance to empower China's legal community.

环球律师事务所
GLOBAL LAW OFFICE

About GLO - The First Chinese Law Firm

First law firm in China: The history of Global Law Office (hereinafter the "GLO") dates back to the establishment of the Legal Consultant Office of China Council for the Promotion of International Trade (hereinafter the "CCPIT") in 1979, when it became the first law firm of China to take an international perspective on its business, fully embracing the outside world. After over 40 years of persistent efforts and development, we have become one of the most prominent large comprehensive law firms in China legal industry.

Among the most prominent large comprehensive law firms in China: GLO has been committing to the mission of "serving domestic and foreign clients with globalized vision, globalized team and globalized quality" since its inception, allowing us to always maintain leading position in the industry in the midst of ever-changing global economic environment. We are proud to be one of Chinese most respected and well-connected law firms, recognized as such by both international and domestic league tables and legal institutions for consecutive years, including the Chambers and Partners, The Legal 500 and Asian Legal Business, etc.

Professional and excellent lawyer team: all lawyers of GLO are graduates from first-tier domestic and/or international law schools, most of whom hold LLM or higher degrees. Many partners have the qualification to practice law in the U.S., UK, Australia, Switzerland, New Zealand, Hong Kong, among others. Our lawyer team has excellent professional backgrounds, and many lawyers have experience of working at courts, domestic and foreign first-tier law firms or leading enterprises and organizations in the industry.

Comprehensive one-stop legal services: we provide comprehensive one-stop legal services for domestic and foreign clients from various sectors and industries. We are committed to a variety of industries, including but not limited to sub sectors such as banking, finance, insurance, securities, investment, trade, energy, mining, chemical engineering, steel, manufacturing, transportation, infrastructure and public facilities, life science and healthcare, telecommunication, media, and high technology, culture, entertainment & sports, real estate, hotel & leisure, catering and large consumption, and etc.

Innovative problem-solving abilities: our lawyers are able to apply practical and constructive comprehensive legal solutions by integrating excellent professional law skills with sophisticated business knowledge so as to solve various complex and fast-changing matters. With leading professional innovative capabilities, we are adept at creatively designing transaction structures as well as details. Over the last three decades, our expertise has helped set the agenda for change through precedents involving many of the country's "firsts".

Client oriented service philosophy: over the past three decades, with profound legal knowledge, extensive practice experience, high professional dedication and strong professional ethics sense, we have demonstrated and proved our values and won trust from domestic and foreign clients. In the future, we will continue to help domestic and foreign clients get enduring and long-term success via our unique advantages.

Authors

Maggie Meng is a Partner of Global Law Office (Beijing Office). She mainly practiced in cybersecurity, personal information security, internet, e-commerce compliance, and anti-corruption and anti-commercial bribery. She previously worked at Fortune 500 companies like Nokia and a well-known law firm for more than ten years. She was also the General Counsel and Data Protection Officer (DPO) of Mobvoi. Maggie has served large multinational companies, well-known network enterprise, automobile companies as well as companies in IoT, telecommunications, cloud services, AI, finance, medical industries and help them build the domestic/international data compliance scheme or provide professional advice on specific projects. During her practice, Maggie has concluded a lot of feasible practical methodlogy which is highly endorsed by the clients. Maggies is also the co-chairman of IAPP China and rewarded with the "Legal 500- the specailly recommended lawyer of 2020 in TMT industry," together with "the top 1000 expert lawyers for the foreign affairs" by the China Lawyers Association. She has translated the data protection laws of the US, Europe, India, Brazil, Russia and other countries, and has authored hundreds of academic articles and books on major magazines, newspapers, and WeChat official accounts, such as White Paper of SDK Security and Compliance (V1.0 & V2.0) and Personalised Dislay Securtity and Compliance Report.

Koh Kok Shen is a senior consultant of global law firm. He has more than 20 years of experience in the commercial and compliance field of telecommunications, IT and financial services. He is familiar with U.S. compliance law and justice department practices and has a deep knowledge of cross-culture legal compliance issues and cooperation. Mr. Koh was formerly the Asia Pacific Compliance Director at Diebold Inc. and China Compliance Director Nokia, Mr. Koh has also many years of experience leading commercial negotiations in Asia. He is admitted to both the UK and Singapore Bar. Mr. Koh was also practice law in Singapore where he advised internet companies and start-ups on internet and IT law for many years for many years before relocating to China in 2005.

Wang Cheng is an Associate of Global Law Office. She mainly practices in data compliance, intellectual property and dispute resolution. She previously worked at the legal department of Citibank and practiced in New York state as a litigation attoreny. She is qualified to practice law in the State of New York and in the Federal District Court for the Northern District of New York. Ms. Wang graduated from Shanghai International Studies University and the Law School of Emory University where she respectively received her bachelor degree of laws and master degree of laws.

Chen Ziqian is a Paralegal at Global Law Office. He has rich experience in cybersecurity, data compliance, and personal information protection areas. He has been responsible for legal research on data compliance, and has published many academic articles on data protection law in various countries while doing internship at Mobvoi. Mr. Chen graduated from Southwest University of Political Science, and is able to work in Chinese and English.

Zhang Shuyi is a Paralegal at Global Law Office. She has rich experience in the field of cybersecurity, data compliance, and personal information protection. She has published many articles regarding the analysis of data protection laws. Ms. Zhang graduated from China Foreign Affairs University and the University of Edinburgh, and received bachelor degree of laws.

Special Thanks to:

Liu Shujun, Yin Kun, Shi Xiaowei, Liu Xinyi, Ye Ouyi, and Wang Ruohan.

Bird & Bird

About Bird & Bird

Bird & Bird is a truly international firm, organised around our clients. We match our passion and practical expertise to your vision to achieve real commercial advantage.

Everything is connected.

With more than 1,350 lawyers and legal practitioners across a worldwide network of 29 offices, Bird & Bird specialises in delivering expertise across a full range of legal services. Our specialisms include advising on commercial, corporate, EU and competition, intellectual property, dispute resolution, employment, finance and real estate matters.

The key to our success is our constantly evolving sector-focused approach. Our clients build their businesses on technology and intangible assets, and operate in regulated markets. To better meet their needs we have developed deep industry understanding of key sectors, including automotive, aviation & defence, energy & utilities, financial services, life sciences & healthcare, retail & consumer, media, entertainment & sport and tech & comms.

International reach

Bird & Bird has offices in key business centres across the globe:

- Europe: Amsterdam, Bratislava, Brussels, Budapest, Copenhagen, Düsseldorf, Frankfurt, The Hague, Hamburg, Helsinki, London, Luxembourg, Lyon, Madrid, Milan, Munich, Paris, Prague, Rome, Stockholm and Warsaw.
- Middle East & Asia: Abu Dhabi, Beijing, Dubai, Hong Kong, Shanghai, Singapore and Sydney.
- North America: San Francisco

We were the first truly international firm with a presence in Denmark, Finland and Sweden, ideally positioning us to support companies looking to invest in the Nordic region. Additional focus groups for Africa, India, Japan and Russia, and extensive cooperation agreements with local firms increase our reach to other key jurisdictions. We have recently opened a representative office in San Francisco to support our US clients with their non-US legal needs.

Excellence in client service

Bird & Bird operates as one truly international partnership: our goals, accounting and profit pool are all shared, as is our commitment to providing our clients with advice from the right lawyers, in the right locations. Our open and flexible business culture allows us to configure ourselves to respond as quickly and effectively as possible to the commercial pressures faced by our clients. Our priority is providing excellent client service, however they themselves define excellence.

Deep industry knowledge

- Expertise in the legal and regulatory framework relating to each sector.
- A more practical, commercial approach, supported by advisors with decades of experience working in the relevant industries

China Contact

Ted Chwu - Greater China Managing Partner; ted.chwu@twobirds.com

环球律师事务所 GLOBAL LAW OFFICE SINCE 1979

Experts and Counsels:

Ruth Boardman
Partner, London
ruth.boardman@twobirds.com

Michelle Chan
Partner, Hong Kong
michelle.chan@twobirds.com

Hamish Fraser
Partner, Sydney
hamish.fraser@twobirds.com

Ariane Mole
Partner, France
ariane.mole@twobirds.com

Dr. Fabian Niemann
Partner, Germany
fabian.niemann@twobirds.com

Jeremy Tan
Partner, Singapore
jeremy.tan@twobirds.com

Lupe Sampedro
Partner, London
lupe.sampedro@twobirds.com

Berend Van Der Eijk
Associate, Netherlands
berend.vandereijk@twobirds.com

Clarice Yue
Counsel, Hong Kong
clarice.yue@twobirds.com

Lisa Vanderwal
Counsel, Sydney
lisa.vanderwal@twobirds.com

Dr. Lena El-Malak
Associate, UAE
lena.elmalak@twobirds.com

Dr. Natallia Karniyevich
Associate, Germany
natallia.karniyevich@twobirds.com

Chester Lim
Associate, Singapore
chester.lim@twobirds.com

Willy Mikalef
Associate, France
willy.mikalef@twobirds.com

Tiantian Ke
Associate, Shanghai
tiantian.ke@twobirds.com

Ester Vidal
Associate, Spain
ester.vidal@twobirds.com

NISHIMURA & ASAHI

About Nishimura & Asahi

The merger of several Top law firms that evolved into a firm capable of providing a full range of legal services. Nishimura & Asahi evolved into its present form through the integration of several diverse law firms each offering highly specialized services. By utilizing each other's strengths, experience and knowledge, Nishimura & Asahi have expanded our areas of expertise and enhanced our ability to act swiftly, giving us the capability to handle any unforeseen changes in the socio-economic circumstances or legal systems.

Over 600 lawyers, the largest law firm in Japan. Our firm comprises over 600 Japanese and foreign lawyers, with a total number of members exceeding 1,600 including licensed tax counsel, patent attorneys, paralegals, and support staff. Each member of the firm possesses diverse specialized skills and can handle a broad range of legal areas. Their abilities form the collective strength of Nishimura & Asahi.

Building a solid network to meet the challenges and opportunities of globalization. As experts in international law, Nishimura & Asahi has created a network covering many countries in Europe, the United States, and beyond. Since 2010, Nishimura & Asahi have opened offices in various countries, starting with Asia, as Japanese corporations have adopted new overseas expansion strategies. At the same time, Nishimura & Asahi have established close affiliations with major law firms overseas, enabling us to provide legal services tailored to the laws and circumstances of those countries. Nishimura & Asahi have also opened three additional offices in Japan to support our clients from various locations within Japan to expand overseas. As a consequence, Nishimura & Asahi have a flexible structure to address diverse global business issues.

About Personal Data & Privacy/Big Data Businesses

With the rapid evolution of information technology, companies are increasingly making use of big data. However, such utilization is a cause for concern for many individuals. Accordingly, many countries and jurisdictions, including Japan and the EU, recognize the importance of protecting personal data and privacy, and have implemented legislation restricting the use of data in certain circumstances. Nishimura & Asahi follows the latest developments in this area, analyzes them from a holistic perspective and provides practical advice relating to the utilization of personal data and other data in various contexts, including the financial, medical, IT and other industrial sectors. Nishimura & Asahi also has considerable experience in advising clients in cases of data breach, privacy infringement or other similar incidents, as well as cybersecurity. In the case where other countries or jurisdictions are involved, Nishimura & Asahi collaborate with local counsel in the respective countries and jurisdictions.

Nishimura & Asahi - Data Privacy Practice Group Contact :
Yuko Kawai (partner)
y_kawai@jurists.co.jp

Contents

Perface

The "Guidelines for the Protection of Personal Data Privacy and Cross-border Flows" published by OECD has proposed to encourage the free data flows while promoting the trade flows (except for special circumstances). In this way, a balance of interests for all parties may be achieved by establishing a common standard for cross-border data flows to improve the "interactivity" of global privacy regulations. The "Comprehensive Progressive Trans-Pacific Partnership" emphasizes that data shall flow freely along with free trade in goods and services. As a symbol of the current digital society and information age, the emergence of the "digital economy", the progress of the "Belt and Road" strategy, network patterns are being created whereby China is more closely associated with the world. Data has been firmly established as a core asset driving future economic growth and efficiencies, which has become an element of new productivity together with "oil, minerals, natural gas, and etc.".

There is an increasing occurance of cross-border acquisitions, overseas investments, cross-border e-commerce and after-sales support, cross-border payments and logistics, and global versions of applications, which rely on data collected from the all over the world for analysis, calculation, and decision-making. Large multinational enterpries manage and operate their global business and employees in a unified manner. Services will be procured locally or outsourced to overseas third-parties. Cross-border data transfer is suppoted by the deployment of global data centers and participation of third-country cloud service partners. At the same time, the need for greater privacy and data protection has received increasing recognition. Since the European "General Data Protection Regulation" ("GDPR") came into force, legislation on privacy and data protection in many jurisdictions have been developing rapidly and vigorously.

This " Globalization and Privacy Protection Guide" is divided into four parts. From the perspective of the companies in China who plan to expand to overseas , this Guide will will provide practical compliance guidelines and introduce (1) the current challenges and opportunities under data globalization that are encountered by companies, (2) how to pre-plan for their overseas business (including sorting out the requirements for data exportation and inventory of such data, drafting and assessing contracts, accomplishing special approval procedures and determining target jurisdictions, etc.), (3) interpretation of data and privacy protection laws in key target jurisdictions and regions, and (4) an overview of the cross-border data flow systems among regions.

From this Guide, it can be noted that some laws have been largely inspired by and designed to align with the GDPR, while others take a different approach to serve their specific needs.

Except for special categories of data that are subject to data localization, cross-border data transfer is in principle allowed in most jurisdictions, while some prescribe different conditions for cross-border data transfer due to their national conditions: in some jurisdictions, data exportation is basically allowed while special categories of data are prohibited to be exported abroad; while in some jurisdictions, data exportation is prohibited in principle and is only permitted in exceptional cases.

For domestic companies which plan to go overseas and foreign companies that are expanding into China, we present thisGuide to provide a reference so as to assist them in learning the privacy protection laws and regulatory policies in various jurisdictions in advance. In this way, these companies may avoid oversight while trying to localize or globalize their operations. Meanwhile, we also expect a comprehensive, high-level, and multilateral cooperation framework in data privacy to be built among different jurisdictions, to explore the compatibility of privacy protection laws and regulations and their implementation. Only with consistency can the digital economy advance in a harmonious, sufficient, and orderly manner. A multilateral win-win situation will then be ensured on the basis of national security. According to Article 12 of "Personal Information Protection Law (Draft)", China shall actively participate in the formulation of international rules for personal information protection, promote international exchanges and cooperation, and promote mutual recognition with other countries, regions and international organizations regarding rules and standards to protect personal information. It is also one of our motives if this Guide may contribute ideas and information to the academies and legislation.

It will be our honor if we may receive comments from peers and friends and thank you for staying with us all the way!

Maggie Meng
Written in the early morning of November 8, 2020,
Tower 1, China Central Place
(Email: mengjie@glo.com.cn)

Copyright: Global Law Office reserves all rights to the report. Without the written permission of Global Law Office, no one shall copy or reprint any copyrighted content of this report in any form or by any means.

Disclaimer: This report does not represent the legal opinions of Global Law Office on related issues. Whoever makes action or omission decisions only in accordance with all or part of the report content shall bear the consequences resulting therefrom. If you need legal advice or other expert advice, you should contact us or a qualified professional.

Part I
Data Globalization – Challenges and Opportunities for Businesses

I. Trends and Developments

In the digital society and information age, data has been firmly established as a core asset driving future economic growth and efficiencies, along with the increasing recognition of privacy and data protection.

The coming into force of the EU General Data Protection Regulation ("GDPR") - the EU's cornerstone data protection law - has not only changed the landscape in Europe, but also served as the global reference point for privacy and data protection laws, shaping legislation worldwide. Following the EU stance, a wave of new privacy and data protection legislation in the US, China, India, Southeast Asia, and many other regions has emerged. Some laws have been largely inspired by and designed to align with the GDPR, while others take a different approach that serves the need of their jurisdictions.

As privacy and data protection regimes across the globe have developed, we can see a number of common features, including broader territorial and exterritorial application, stepped-up enforcement or sanction provisions, stronger protection for data subject rights, and rising awareness of national and cyberspace sovereignty. Privacy and data protection law is expected to continue to be one of the most dynamic and fast-evolving areas of law over the next few years.

II. Challenges for Businesses

As privacy and data protection laws and regulations surge across the globe, nearly all businesses are struggling to effectively address the multi-faceted and broad range of regulatory and operational risks associated with the data lifecycle, including the collection, use, sharing and disclosure, and otherwise processing of data. Some primary challenges for businesses are further set out below.

1. No "all-in-one" method for businesses' data protection compliance worldwide. Though most recent updates to privacy and data protection regimes have been inspired by the GDPR to an extent, merely aiming to comply with the GDPR will be insufficient for a global compliance strategy because local variations will need to be taken into account. Even among European countries, the GDPR does not fully harmonise the rules – it allows EU Member States to legislate on certain data protection matters. Meeting such country-specific derogations can be viable, but businesses should get ready to comply with increasingly stringent local requirements.

2. Cross-border data transfer is facing increasing difficulties. Despite the benefits for businesses, consumers, and national economies benefit from the free flow of data across borders, many countries have erected barriers to cross-border data flows, such as data localization requirements that prohibit or restrict certain or all data export. Businesses should be equipped with a good understanding of the applicable data export regulations in the jurisdictions where their businesses operate.

3. Enforcement under the data privacy law is making headlines. Non-compliance with privacy and data protection laws may result in a range of damaging consequences for an organization, including large monetary fines, reputational damage, loss of customer trust, and consumer or employee group and individual actions etc. In addition, a crippling data breach could greatly affect the successful and continuous operation of a business.

4. Emerging technology and innovation may encounter legal challenges from privacy and data protection laws. There is a tension between new technology and privacy and data protection law when the precise impact of the technology is hard to anticipate with certainty. It could be challenging for businesses to find a way to develop and adopt such new technology data-privacy-compliant manner.

To help businesses navigate through various privacy and data protection requirements among different jurisdictions, we are pleased to present this Guide of Data Globalization and Privacy Protection.

In the following sections, this Guide will introduce the privacy and data protection regimes in a number of jurisdictions, including

• Europe (including the U.K., Germany, France, the Netherlands, and Spain)

• North America (including U.S., Canada)

• Asia (including Japan, China, Hong Kong (China), Macao (China), Taiwan (China), Singapore, Malesia, Thailand, India, United Arab Emirates, Saudi Arabia) and

• Oceania (Australia and New Zealand).

For each jurisdiction, we summary typical questions that have been frequently asked by companies about privacy and data protection laws, i.e.

• How does the legal system of data protection work in a certain jurisdiction?

• Who is/are responsible for supervision and enforcement of the law?

• How does the law apply to my company?

• What are the data protection principles?

• What legal basis can my company rely on?

• How is personal data defined?

• When is my company a controller or a processor?

• What rights does a data subject have?

• What information should be provided in a privacy notice?

• What direct marketing regulations should my company be aware of?

• What are the requirements for data sharing and processing?

• Is there any special protection for children's data?

• What measures should my company adopt to ensure accountability?

• Is there a requirement for data breach notification?

• What are the cross-border data transfer rules?

• How is the data privacy law enforced in a jurisdiction?

Part II
Preliminary planning for China's companies going global

I. Data Compliance of Cross-Border Commerce for Business

As the core of the cybersecurity legal system at this stage, the Cyber Security Law of China only restricts the cross-border transfer of personal information and important data collected and generated by Critical Information Infrastructure Operators within the territory of China. Simultaneously, the restrictions for "general" network operators are not explicit, and other current laws and regulations restrict data cross-border transfer in certain industries.

China has imposed stricter restrictions on the data cross-border transfer from the drafts for comments of various regulations or national standards. Through clear and reasonable regulations, data can be transferred in an orderly and safe manner without infringing cyberspace sovereignty, national security, data security, corporate and individual rights. The recently issued the Data Security Law (Draft) also bears this out. Articles 1 and 2 of the draft clarify the promotion of data mining and utilization, but if data activities carried out by overseas organizations or individuals harm national security, public interests, or the rights and interests of citizens or organizations, they will be held liable in accordance with the law. This provision shows the legislative purpose of not only encouraging data circulation but also safeguarding national security and data sovereignty, which endows the Data Security Law (Draft) with necessary extraterritorial effects. The second paragraph of Article 3 of the Personal Information Protection Law (Draft) issued in October 2020 also clearly stipulates that this law shall apply to the processing of domestic personal information outside China when providing products or services to domestic individuals, or apply to the analysis and

evaluation of the behavior of domestic individuals.

Therefore, data cross-border transfer is not strictly prohibited or difficult to achieve under the current Chinese legal system compared with other countries. Businesses can export data after fulfilling the corresponding compliance obligations. Businesses should pay attention to the following points before planning data cross-border transfer.

1.Clarify the Company's Business Types and Data Collection

1.1 Data Localization

According to Article 37 of the Cyber Security Law, personal information and important data collected and produced by critical information infrastructure operators during their operations within China's territory shall be stored within China. Only when necessary for business requirements can the data be cross-border transferred after being evaluated by relevant regulatory authorities. Article 40 of the Personal Information Protection Law (Draft) on critical information infrastructure operators is basically consistent with Article 37 of the Cyber Security Law. However, the data localization threshold has been raised; that is, where the personal information obtained reaches a certain amount, the personal information shall be stored in China. The cyberspace authority may issue specific requirements on this requirement in the future.

If the company meets the criteria of a Critical Information Infrastructure Operator, and after the evaluation, it is confirmed that the data cross-border transfer is "indeed required." In that case, the self-assessment must be kept for two years and reported to the relevant administrative department. Therefore, businesses should make advance preparations and evaluate their business in a timely manner. They should clarify whether they will be deemed a Critical Information Infrastructure Operator and pay attention to the amount of personal information they process to ensure the compliance of their data cross-border transfer. According to documents such as the draft for comments issued recently, general network operators should also conduct self-assessment in advance. However, unlike critical information infrastructure operators, network operators only need to be evaluated by the regulatory authority when they meet particular conditions. In other cases, they can complete the evaluation by themselves. Although such regulations have not yet come into effect and have no binding force, they represent the legislature's attitude on data cross-border transfer. These draft regulations will likely come into effect in the near future. Therefore, businesses should develop an evaluation system for data cross-border transfer as soon as possible.

1.2 Data Type

According to the Law of the People's Republic of China on Guarding State Secrets and relevant laws, regulations, and national standards, not all data can be transferred cross-border. There are specific restrictions on certain data cross-border transfer. To complete

cross-border commerce, businesses should fully consider business scenarios, types of data, and data restrictions in their planning before conducting data cross-border transfer to avoid obstacles and violations of relevant laws and regulations and reduce unnecessary losses.

1.2.1 Types of restricted data for cross-border transfer

	Laws and Regulations	Data Type	Restriction for Data Cross-border Transfer
1.	Law of the People's Republic of China on Guarding State Secrets	State Secret Data	Prohibits cross-border transfer
2.	Regulation on Map Management	Map Data	Requires servers to be located in China
3.	Regulation on the Administration of Credit Investigation Industry	Data Collected by Credit Agencies in China	Information collected by credit agencies in China should be sorted, stored, and processed in China.
4.	Notice by the People's Bank of China Regarding the Effective Protection of Personal Financial Information by Banking Institutions	Personal Financial Data	The personal financial data collected in China should be stored, processed, and analyzed in China. Except as otherwise specified by laws and regulations and the People's Bank of China, banking financial institutions shall not conduct cross-border transfers of domestic personal financial data.
5.	Interim Measures for the Administration of Online Taxi Booking Business Operations and Services (2019 Amendment)	Personal Data and Business-Generated Data	Personal data and business-generated data should be stored and used in mainland China for no less than two years. Unless otherwise provided by laws and regulations, the data mentioned above shall not be transferred abroad...
7.	Measures for the Administration of Population Health Information	Population Health Information	Entities in charge must not store population health information in any server outside China and may not host or lease any server outside China.

8.	Interim Measures for the Management of Human Genetic Resources	Human Genetic Resources	Without permission, no entity or individual is allowed to gather, collect, trade, export, supply cross-border or by other means important genetic pedigrees and genetic resources of specific regions.
9.	Measures for the Administration of National Health and Medical Big Data Standards, Security and Service (Trial)	Health and Medical Big Data	Health and medical big data shall be stored on a secure server in China. If data needs to be transferred cross-border due to business needs, a security assessment review shall be conducted in accordance with relevant laws, regulations, and requirements.
10.	Measures for the Administration of the Real-Name Receipt and Delivery of Mails and Express Mails	User information and important data collected and generated during sending and receiving activity using real names	User information and important data collected and generated by a delivery enterprise during the real-name receipt and delivery activities in China shall be stored in the territory of China.
11.	Measures for the Administration of Information Technology Management of Securities Fund Trading Institutions Measures for the Administration of Foreign-Funded Futures Companies Measures for the Administration of Private Investment Fund Service Business (Trial) Regulation on Strengthening the Confidentiality and File Management Related to the Issuance and Listing of Securities Overseas	Clients' information and business data Work papers and other files created in China by securities companies and securities service institutions that provide relevant securities services	Unless it is otherwise prescribed by any law or regulation or the provision of the CSRC, the securities fund trading institution shall not allow or cooperate with any other institution or individual to intercept and retain the client's information and shall not provide the client's information to any other institution or individual in any form. The core servers of information systems such as transaction, settlement, and risk control, and data equipment for recording and storing client information of a foreign-funded futures company shall be set up in China. In the process of overseas securities issuance and listing, Work papers and other files created in China by securities companies and securities service institutions that provide relevant securities services shall be stored in China.

1.2.2 Personal Information Cross-Border Transfer

1.2.2.1 Authorization and consent of the subject of personal information

The basic principle for Data Cross-Border Transfer is to obtain consent from the personal information subject. According to the Cybersecurity Law of China, network operators shall obtain approval from the relevant right subject of personal information before they "use" personal information, and the term "use" is defined to include "cross-border transmission." Therefore, no personal information can be exported without the authorization of the personal information subject. The provisions in the Measures for the Security Evaluation of the Export of Personal Information and Important Data (Draft for Comment) are more specific. According to this document, the network operators shall inform the personal information subject of the purpose of data cross-border transfer, the scope and content of personal information, the recipient and its nationality or location. Operators cannot export personal information without the consent of the right subject. In addition, before the cross-border transfer of personal information of minors, operators must obtain their guardians' consent. The provisions in the Measures for the Security Evaluation of the Export of Personal Information and Important Data (Draft for Comment) are more specific. According to this document, the network operators shall inform the personal information subject of the purpose of data cross-border transfer, the scope and content of personal information, the recipient and its nationality or location. Operators cannot export personal information without the consent of the right subject. In addition, before the cross-border transfer of personal information of minors, operators must obtain their guardians' consent. According to the Information Security Technology- Guidelines for Data Cross-Border Transfer Security Assessment (Draft for Comment), the explicit consent in the data cross-border transfer process means that the personal information subject should: proactively make a paper or electronic statement by using, for example, written or verbal means; or take an affirmative action autonomously to authorize operators to perform specific processing of their personal information. The Guidelines also lists the situations that can be considered valid consent in practice, including making international and roaming calls, sending international e-mails, and conducting global instant messaging.

The Personal Information Protection Law (Draft) stipulates that when companies transfer personal information to the territory outside China, they should inform individuals of the recipient's identity, contact information, processing purpose, processing method, and types of personal information, and the way for individuals to exercise their rights to overseas recipients. The businesses shall obtain individuals separate consents, that is, the personal information subject should voluntarily and clearly express intention with full knowledge. Strong reminders are required for personal information subjects to be fully aware of the risks as well as careful consideration and affirmative action such as ticking or signing, to ensure that the subject has made a sufficient expression of intention. This process cannot be replaced by general authorization.

The operator may conduct cross-border transfer of personal information without the personal information subject's consent under certain situations, such as emergencies endangering citizens' life and property. However, this situation hardly occurs during daily operations. Therefore, the businesses are recommended to obtain the consent of the subject of personal information when they cross-border transfer personal information.

Businesses should also note that for cross-border transfer of personal information, they should obtain the personal information subject's consent and may also need the competent authority's approval. For details, please refer to section 1.2.2.3 below.

1.2.2.2 Complete and Comprehensive Contract

In addition to consent, signing a cooperation agreement with the data recipient is the second core element for smooth cross-border personal information transfer. Businesses should stipulate data recipients' rights and obligations in contracts to ensure personal information safe and safeguard the legitimate rights and interests of personal information subjects and the enterprise itself.

Firstly, the business should pay attention to itself and the recipient's roles when cooperating under the contract, not only in relation to the distribution of responsibilities in the event of data security incidents but also affects such important aspects the business's internal policies and protection measures.

The relationship between the businesses and the data recipient may be a relationship involving a data controller and the entrusted processor or a relationship involving joint data controllers. This needs to be analyzed according to the specific data collection and processing scenarios specified in the contract. According to Article 3.4 of the Information Security Technology Personal Information Security Specification, a personal information controller is an "organization or individual capable of determining the purpose and method of processing personal information." Therefore, the core point of judging the roles between the enterprise and the data recipient is to confirm whether the data recipient has autonomy in the purpose and method of data use. When the two parties are "joint controllers," the data receiver is able to determine by itself the collection and use of the data. The data receiver is not required to destroy or return the data according to the enterprise's instructions after the data receiver obtains the data. Some data receivers will request to become "joint data controllers" for subsequent development and data realization. Companies should consider their business needs and evaluate the specific type of data involved.

After determining the two parties' roles, the business should focus on the provisions of the Measures for the Security Assessment for Cross-border Transfer of Personal Information (Draft for Comment). It requires companies to clarity the basic situation in contract, such as the purpose, data type for the cross-border data transfer. It also provides specific and

clear regulations on the relief measures of personal information subjects, the responsibilities and obligations of the recipient and the provider and whether the target country's legal environment is appropriate. It is recommended that when a company intends to sign a contract with an overseas data recipient, it should pay attention to the contract clauses mentioned above.

If required by the subject of personal information, the company should provide a copy of the contract. The contract is an essential reference document for the regulatory authority to conduct security assessments. It is therefore recommended that companies pay attention to such agreements and improve the contract terms.

1.2.2.3 Provincial Cyberspace Administrations to Conduct Security Assessments for Personal Information

According to the Measures for the Security Assessment for Cross-border Transfer of Personal Information (Draft for Comment), network operators should report to the local provincial cyberspace administrations for cross-border transfer security assessment of personal information before cross-border transfer of the data. The assessment conducted by the provincial cyberspace administrations is a required procedure for personal information cross-border transfer. Only upon the evaluation and consent of provincial cyberspace administrations, can cross-border data transfer be allowed.

Therefore, it is recommended that companies conduct a self-assessment before proceeding with personal information cross-border transfer to find potential risks and rectify them in time and consequently improve the assessment approval rate by the competent authority.

Consent of the personal information subject is needed for the security assessment. Therefore, businesses can conduct the assessment after confirming the personal information subject's consent. A company should focus on evaluating the following items:

- Whether it has developed a plan for data cross-border transfer
- Whether it complies with national laws, regulations, and policies.
- Whether the contract terms can fully protect the legal rights and interests of the personal information subject.
- Whether the contract can be effectively executed.
- Whether the company or the recipient has a history of infringing the rights and interests of information subjects, and whether the company or the recipient has experienced major network security incidents.

• Whether the company has obtained the personal information legally and properly.

If personal information is allowed to leave the country, the enterprise shall establish a cross-border personal information transfer record and keep it for at least 5 years. At the same time, the enterprise shall report the current year's cross-border personal information transfer situation and contract performance to the local provincial network and information department before December 31 of each year.

It should be noted that the Personal Information Protection Law (Draft) draws on the relevant regulations on SCC and certification in the GDPR to avoid a one-size-fits-all approach. This law stipulates three situations, namely evaluation by the Office of the Cyberspace Administration of China; personal information protection certification conducted by professional institutions, and signing of contracts with overseas recipients. If a business needs to transfer personal information to the territory outside China due to business needs, it shall meet at least any of the above conditions. This change promotes data circulation and provides more choices for companies to transfer personal information cross-border in normal commercial trade.

The Personal Information Protection Law (Draft) marks China's progress in the protection of personal information. Although the draft is currently in the request for comments stage, it still reflects China's trend towards protecting personal information. At the same time, in view of the high costs for non-compliance imposed by the Personal Information Protection Law (Draft), it is recommended that companies conduct self-inspection as soon as possible. Companies should focus on security impact assessments, formulating internal management systems, implementing security measures such as classification and encrypted storage of personal information, determining internal operating rights, recording processing activities, formulating emergency plans, regularly conducting audits and training drills to develop a comprehensive and sustainable cross-border data transfer compliance system.

1.2.3 Cross-border important data transfer

1.2.3.1 Identify data

Based on the Measures for the Administration of Data Security (Draft for comments), the term "important data" means data whose divulgation may directly affect national security, economic security, social stability, public health and security, such as undisclosed government information and extensive population, genetic health, geographical, and mineral resources. Important data shall generally not cover information on the production, operation, and internal management of an enterprise and personal information. The types of important data are listed in Appendix A of Guidelines for Data Cross-border Transfer Security Assessment and should be the main reference for businesses to determine what is important data.

1.2.3.2 Self-assessment

The security impact assessment for important data before cross-border transfer is different from that for personal information. Businesses should conduct self-assessments before personal information cross-border transfer and be responsible for the results of the assessment. During the assessment process, a company should pay attention to the following points:

- The legality, legitimacy, and necessity of data cross-border transfer.
- Basic statistics for personal information, including the amount, scope, type, and sensitivity of personal information, whether the subject of personal information consent for their personal information cross-border transfer, etc.
- Basic statistics for important data, including the quantity, scope, type, and sensitivity of important data.
- The security protection measures, capabilities and level of the data recipient, and the network security environment of the target country and region.
- Risks of data being leaked, damaged, tampered with, abused, etc., after being cross-border transferred and re-transferred.
- Risks of data cross-border transfer and data aggregation to national security, public interests, and individual legitimate interests.

After completing the self-assessment, the business shall retain the self-assessment report for at least two years and conduct at least one self-assessment every year and report the assessment to the industry supervisor or regulatory authority promptly. Although the important data cross-border transfer does not have to be assessed by the administrative and regulatory department, it differs from personal information cross-border transfer. However, according to Article 28 of the Measures for the Administration of Data Security (Draft for comments), the network operator shall, before releasing, sharing, trading, or exporting important data, assess possible security risks resulting therefrom and report to the regulatory authority having jurisdiction over the industry for approval, or in the absence of such regulatory authority, to the provincial cyberspace authority. Therefore, China has increased the control of the authority in data cross-border transfer and holds the principle of transfer data by legally and orderly means.

1.2.3.3 Submission for Competent Authority Assessment

Under particular circumstances, such as where a large volume of data is involved, sensitive data types, and other situations that may endanger national security and public interests, conducting self-assessments is insufficient to meet reasonable security expectations. In

this case, the network operator should submit a request to the competent authority for an assessment. The Cyberspace Administration of China and the competent authority determine the assessment's scope, formulate an assessment plan, establish an assessment working group, and make a competent authority assessment report. The expert committee will review the competent authority assessment report and the self-assessment report and give recommendations on whether to approve data cross-border transfer. Finally, the Cyberspace Administration of China and the competent department will make decisions based on these recommendations.

In this case, the business should conduct a comprehensive self-assessment in advance and make rectifications based on the self-assessment results. To increase the probability of passing the assessment, we recommended that the enterprise ensure that it has adequately addressed the assessment indicators before submitting to competent authority assessment.

2. Reasonably Choose the Target Country

A business should make careful considerations and analysis before choosing the target country for data cross-border transfer. Many factors need to be evaluated to decide, such as customer groups' needs, the cost of data cross-border transfer, and the convenience of the company operations. In addition to commercial considerations, the provisions of Chinese laws, regulations, and national standards for data cross-border transfer should not be ignored, especially the requirements, rules, and restrictions on target countries that are contained in these provisions.

The Guidelines for Information Security Technology – Guidelines for Data Cross-border Transfer Security Assessment (Draft for Comment) (Guidelines for Data Cross-border Transfer Security Assessment) has detailed the requirements for cross-border data transfer security, which provides more specified guidelines for businesses and institutions. Article 5.2.6 stipulates that for the target country, the critical points of the cross-border data transfer security assessment should include "the political and legal system of country or region where the data recipient is located."

After assessing, reviewing, and confirming that the data cross-border transfer requirements are met, companies should focus on the laws, regulations, judicial precedents, and contract requirements of personal information and privacy protection in the target country or region to ensure that data storage, processing, sharing, and transfer in the target country or region comply with local rules.

2.1 The Assessment Requirements of the Target Country

The Guidelines for Data Cross-border Transfer Security Assessment further distinguishes the assessment requirements of the target country. For personal information cross-border

transfer, businesses should evaluate the following aspects of the target country:

- Differences between the current personal information protection laws, regulations, or standards of the target country or region and that of China.
- The regional or global personal information protection mechanisms joined by the target country or region, and the binding commitments made by it.
- The implementation of personal information protection mechanisms in the target country or region. For example, whether there are specific law enforcement or supervision agencies, industry self-discipline system, administrative or judicial relief measures for data subjects, etc.

When the exported data is the important data specified in Appendix A of the Guidelines for Data Cross-border Transfer Security Assessment[1], in addition to the above three aspects, government agencies also should evaluate the following aspects of the target country or region:

- Current laws, regulations, and standards in data security in the target country or region.
- The implementation of the data security mechanism in the target country or region, such as competent departments, judicial mechanisms, industry level self-regulation, in cybersecurity or data security.
- Countries or regions' bilateral or multilateral agreements on data transferring and sharing.

2.2 Evaluation results

According to the Article B.3.3 in Appendix B of the Guidelines for Data Cross-border Transfer Security Assessment, the laws of the target country or region is classified into three levels of protection capability (high, medium, and low) according to specific conditions and are regarded as the basis for assessing the overall security risk level of the target country or

1 That is, data, excluding state secrets, collected and generated by relevant organizations, institutions and individuals within the territory and closely related to national security, economic development, and public interests (including raw data and derivative data). Once the data is disclosed, lost, abused, tampered, destroyed, aggregation, integration, or analysis without authorization, which may cause the following consequences, the data should be deemed important data:
a) Endanger national security, national defense interests, and disrupt international relations.
b) Damage to national property, public interest, and individual rights.
c) Influencing the country to prevent and combat economic and military espionage, political infiltration, organized crime, etc.
d) Influencing administrative agencies to investigate and handle illegal, dereliction of duty, or suspected illegal or dereliction of duty according to law.
e) Interfering with administrative activities such as supervision, management, inspection, and auditing carried out by government departments in accordance with the law and hindering government departments from performing their duties.
f) Compromise the system security of critical infrastructure, critical information infrastructure, and government information systems.
g) Affect or endanger national economic order and financial security.
h) State secrets or sensitive information can be analyzed from the data.
i) Affect or endanger other national security issues such as national politics, territory, military, economy, culture, society, science and technology, information, ecology, resources, nuclear facilities, etc.

region.

The overall security risk level of a target country or region may also significantly impact the process of data cross-border transfer. Therefore, before selecting a target country or region, businesses should analyze their business returns and the cybersecurity legal systems of the target country to ensure that the data security risks of the country are controllable, so that the data can be transferred smoothly. If the risk is uncontrollable, it means that the protection measures for the target country or region's data security are insufficient. If the businesses still decide to transfer data to the target country, it may suffer losses caused by data security incidents and may even be punished by relevant government departments.

3. Being familiar with the laws, regulations, judicial precedents, and contract requirements of the target country or region

After assessing, reviewing, and confirming that the data cross-border transfer requirements are met, companies should focus on the laws, regulations, judicial precedents, and contract requirements of personal information and privacy protection in the target country or region to ensure that data storage, processing, sharing, and transfer in the target country or region comply with local rules.

With the rapid development of the digital economy and big data, countries are actively exploring the regulatory system to realize the commercial value of data without harming personal information subjects' rights. The major target countries or regions for domestic businesses are the European Union, the United States, and the Asia-Pacific region. These jurisdictions have already issued laws for data protection. For example, the EU's General Data Protection Regulation (GDPR) and opinions and guidelines issued by EDPB have established a new legal system for data protection in the EU with unified protection standards; the United States has not made a unified data protection law at the federal level, but it has adopted specific regulations for certain types of data for various industries in different regulations, such as the COPPA for child protection, the HIPAA for the medical field, etc. Laws for personal information protection and privacy are being implemented at the state level, such as the California Consumer Privacy Act (CCPA), which regulates the collection and processing of personal information from the perspective of consumer protection, clarifying data protection rules and obligations to subjects. Countries in the Asia-Pacific region also generally attach importance to personal information protection and privacy security issues and have issued laws, such as South Korea's Personal Information Protection Act (PIPA), India's Personal Data Protection Bill (PDPB).

Companies that violate the laws mentioned above will bear relatively severe liabilities and consequences. It is recommended that companies should pay attention to the personal information protection laws, regulations, and policies of the target country in advance and complete the follow-up processing procedures legally and compliantly after the data goes abroad to prevent or reduce unnecessary losses. For details, please refer to the analysis of

the personal information protection laws and regulations of different countries and regions in this Guide's remaining chapters.

II. Conclusion

1. Establish a compliance system

To sum up, operators must carry out a series of considerations and evaluations before conducting data cross-border transfer. Firstly, operators should analyze the business and data involved in overseas trade and determine the target country. Secondly, operators should evaluate data cross-border transfer's purpose and confirm the legality, legitimacy, and necessity of data cross-border transfer. Thirdly, operators should complete data cross-border transfer plans and carry out data security self-assessment. If necessary, operators should obtain the approval of the national cyberspace administration and competent authority. Even if the compliance system has satisfied all legal requirements, operators should identify their role during data collection and processing and take adequate measures to protect user data. Also, the compliance work of the target country cannot be ignored. For operators, ensuring data security can reduce unnecessary penalties for violations.

Therefore, operators should establish a standardized compliance system with complete procedures and documents for the data cross-border transfer, including but not limited to online agreements, self-assessment process templates, internal security protection systems, and cooperation agreement templates for cross-border data transfer. Operators should also complete regular self-assessments and fulfill reporting obligations to ensure that the process of data cross-border transfer is safe, controllable, and legally compliant.

2. Continuous compliance: monitor and adjust

It should be noted that data cross-border transfer compliance is a continuous and dynamic process. The operators should establish a data cross-border transfer compliance system and monitor updates of related laws and regulations, changes in the data types, purposes, and recipients of data cross-border transfer. A long-term monitoring system is crucial for operators which includes: self-assessments for security protection capabilities, assessments for data security protection capabilities of the data recipient, the monitoring for laws, regulations, and the political environment of the target country. Operators should promptly adjust the data cross-border transfer compliance system according to the requirements of relevant laws and regulations after any change of monitored elements. Continuous compliance is the key to control the risk of data cross-border transfer within a controllable range for operators.

Part III
Global Data Protection and Privacy

I. Europe

1.GDPR Overview

1.1 Overview

1.1.1 Legal System

The EU General Data Protection Regulation ("GDPR")[2] replaced the EU Data Protection Directive[3] and all data protection laws of member states when it became applicable from 25 May 2018. It is a law with the nature of "regulation." As a Regulation, the GDPR is directly, unitively, and primarily effective in Member States without the need for implementing legislation. However, on numerous occasions (e.g. compliance with a legal obligation, performance of a public task, employee data processing), the GDPR allows/ requires Member States to legislate on data protection matters.

In addition to the GDPR, other legislation is also of importance for organisations under the EU regime, including, for example, i) the e-Privacy Directive[4] as amended which applies to the processing of personal data in the electronic communications sector, and ii) the

2 Regulation (EU) 2016/679

3 Directive 95/46/EC

4 Directive 2002/58/EC

Law Enforcement Directive[5] which applies to personal data processing by criminal law enforcement authorities for law enforcement purposes.

1.1.2 Supervisory Authorities

Local data protection authorities ("DPAs") in each EU member state continue to exist and to enforce data protection law. These are referred to in GDPR as supervisory authorities. The European Data Protection Board ("EDPB") is an independent EU body responsible for issuing guidelines and providing advice on matters relating to the GDPR. The EDPB also has a role in ensuring consistency between its member DPAs; it has to issue opinions on certain activities undertaken by the DPAs and, in the event of disputes between DPAs, it has a dispute resolution role. The DPAs of all EU member states participate in full in the EDPB. The DPAs of European Economic Area states (Norway, Iceland, and Liechtenstein) participate in a more limited way. The European Data Protection Supervisor ("EDPS") is also a member of the EDPB. The EDPS is responsible for monitoring the application of data protection rules within European Institutions.

1.1.3 Material and Territorial Scope

a) Material Scope

The GDPR applies to the processing of personal data by i) wholly or partly by automated means, or ii) other than by automated means, which form part of or are intended to form part of a filing system, except those that are:

- outside the scope of EU law (e.g. activities concerning national security);
- in relation to the EU's common foreign and security policy;
- carried out by competent authorities for criminal law enforcement purposes (where a separate Directive applies);
- carried out by EU institutions (where a separate Regulation applies);
- carried out by a natural person as part of a "purely personal or household activity". (Art.2, GDPR)

b) Territorial Scope

The GDPR can apply to an organization in two types of ways:

5 Directive (EU) 2016/680

- Establishment Criterion: GDPR applies to an organization which has an EEA "establishment", where personal data are processed "in the context of the activities" of such an establishment. (Art.3(1), GDPR)

- Targeting or Monitoring Criterion: Non-EEA established organizations will be subject to the GDPR where they process personal data about individuals in the EEA in connection with:

• the "offering of goods or services" (payment is not required); or

• "monitoring" their behavior within the EEA. (Art.3(2), GDPR)

The EDPB clarifies that, i) it should be apparent that organizations intend to offer goods or services - (e.g. using an EEA language or EEA currency on its website), and ii) monitoring suggests that the controller is doing this to achieve a purpose (e.g. behavioral advertising and geo-localization of content, online tracking through cookies and device fingerprinting). The monitoring criterion applies whether or not the organization intends to monitor someone in the EEA.

1.1.4 Data Processing Principles

GDPR sets out seven data processing principles, i.e. i) lawfulness, fairness, and transparency, ii) purpose limitation, iii) data minimization, iv) accuracy, v) storage limitation, vi) integrity and confidentiality and vii) accountability. The accountability principle is a newly added one which requires organizations to be responsible for, and be able to demonstrate data compliance. (Art.5 GDPR) Please refer to Section viii "Accountability" below for further analysis on the accountability principle.

1.1.5 Lawful basis for processing

In order for processing of personal data to be allowed under the GDPR, data controllers must have a legal basis for each purpose of processing:

- Consent of the data subject. Consent must be specified, informed, distinguishable, revocable, granular, and otherwise freely given – in other words, the data subject must not experience a detriment if she or he does not give, or revokes, consent.

- Necessary for the performance of a contract with the data subject or to take steps preparatory to such a contract. Processing must be necessary for the entry into or performance of a contract with the data subject.

- Necessary for compliance with a legal obligation under Member State or EU law. A legal obligation need not be statutory, but it should be clear and precise with foreseeable application.

- Necessary to protect the vital interests of a data subject or another person where the data subject is incapable of giving consent, e.g. emergency treatment, disaster response.

- Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

- Necessary for the purposes of legitimate interests. This can be the most flexible legal basis for data controllers, e.g. processing for direct marketing purposes or preventing fraud. Data controllers have to identify what "interest" that they are pursuing; ensure this is legitimate; and balance this against the impact of the processing on individuals. This legitimate interest assessment should be documented. (Art.6, GDPR).

1.2 Key Definitions

1.2.1 Personal Data and Special Categories of Personal Data

Personal data is defined as "any information relating to an identified or identifiable natural person"; a person may be identified in a wide variety of ways such as a name, an identification number, location data, an online identifier etc. (Art.4(1), GDPR)

Special Categories of Personal Data include: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life and sexual orientation, genetic data, and biometric data where processed to uniquely identify a person. (Art.9(1), GDPR) In addition, processing data relating to criminal convictions and offences are restricted similarly to special categories of data. GDPR only permits the processing of special categories of personal data if certain specifically listed exceptions apply, e.g. explicit consent, employment and social security and social protection under EU or Member State law, etc.

1.2.2 Controller and Processor

A controller is a "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". (Art. 4(7), GDPR).

Processors are those who process "personal data on behalf of the controller". Employees are not processors. (Art. 4(8), GDPR).

Please refer to Section vi "Data Sharing and Processing" below for more discussion on the relationship between controllers and processors.

1.3 Data Subject Rights

GDPR substantially extends data subject rights with respect to their personal data including:

- Rights to information and access (i.e. to obtain a copy);
- Right to rectification of inaccuracies in personal data;
- Right to erasure of personal data where the processing fails to satisfy the GDPR requirements (e.g. processing is no longer necessary; the individual withdraws consents; unlawful processing, etc.);
- Right to data portability, i.e. to receive the personal data concerning him or her, which he or she has provided to the controllers, in a structured commonly used and machine readable form, and to transmit those data to another controller without hindrance or to have the data transmitted directly from one controller to another (where technically feasible), where the processing i) is carried out by automatic means, ii) is based on consent or to perform a contract;
- Right to restriction when the processing is challenged (e.g. data accuracy is disputed, or an individual has objected to the processing, etc.);
- Right to object to specific types of processing, including direct marketing (absolute right), processing based on legitimate interests or public tasks and research or statistical purposes.
- When it comes to solely automated decision making, including profiling, with legal effects or similarly significant, on the data subjects, the data subjects have additional rights not to be subject to such decision.
- The right to lodge a complaint with the competent DPA.

The controller must comply "without undue delay" and "at the latest within one month", although there are some possibilities to extend this and, requests to exercise data subject rights could be limited in certain circumstances (e.g. right to access should not adversely affect others, including the protection of intellectual property rights and trade secrets etc.; right to erasure does not apply if processing is necessary for the exercise of the right of freedom of expression or compliance with legal obligation etc.). Additionally, data subject requests should be responded to free of charge.

1.4 Privacy Notice

A Privacy Notice (often also referred to as a Privacy Policy) is an information notice that should be given to data subjects', to meet their right to information and to ensure

transparency of processing. The GDPR requires extensive information to be provided to data subjects "in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child", including for example:

- Identity and contact details of the controller;
- Purposes of processing and legal basis for processing;
- Where special categories of data are processed, the lawful basis should be specified;
- Recipients or categories of recipients;
- Details of data transfers outside the EU;
- The data retention period (or if not possible, the criteria used to set this);
- Data subject rights;
- Whether there is a statutory or contractual requirement to provide the data and the consequences of not providing the data;
- If there will be any automated decision taking, information about the logic involved and the significance and consequences of the processing for the individual; and
- In case of indirect data collection, the categories of information and sources of information.

(Articles 13 and 14 of the GDPR).

1.5 Direct Marketing

Legal basis: Consent and legitimate interests are the legal bases most likely to be relied on under the GDPR to justify direct marketing. For direct marketing by email, the EU e-Privacy Directive mandates opt-in consent for almost all kinds of electronic direct marketing. However, "in the context of the sale of a product or a service" marketing email may be sent with the opt-out mechanism subject to more limited conditions for the direct marketing. Where direct marketing is based on cookies, or other techniques which involve the storage of information on, or the retrieval of information from, a device which is being used on a public electronic communications service, then consent is also required for this. As a result, consent is needed for online behavioral advertising.

Right to object: Under the GDPR, data subjects have the absolute right to object to processing for purposes of direct marketing, or profiling for purposes of direct marketing, which must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".

1.6 Data Sharing and Processing

GDPR imposes a high duty of care on controllers in engaging data processors. Processing by a processor shall be governed by a written contract that sets out a range of information (e.g. the data processed and the duration for processing) and obligations (e.g. assistance where a personal data breach occurs, appropriate technical and organizational measures taken and audit assistance obligations). This also applies where a processor further engages a sub-processor. (Art.28, GDPR). The controller must also check the ability of the processor to meet its obligations.

GDPR also sets out requirements for joint-controllership, i.e. two or more controllers who jointly determine the purpose and means of processing. Joint-controllers are required to arrange between themselves their respective responsibilities for compliance with the GDPR, particularly the exercise of data subject rights and provision of transparency information to individuals. The arrangement must set out the parties' roles and responsibilities with respect to data subjects, and the essence of the arrangement must be made available to data subjects. (Art.26, GDPR)

1.7 Children's Privacy Protection

GDPR sets out a number of child-specific provisions. For example, if an organization offers information society services directly to a child (broadly, online services) and if the lawful basis for processing the child's data is consent, then the organization has to obtain parental consent. In this context, a child is someone under the age of 16 (while Member State may provide by law for an age as low as 13); information notices addressed to children must be child-friendly; processing child data may trigger the need for the Data Protection Impact Assessments, etc. In these latter cases, the child means anyone under 18.

1.8 Accountability

1.8.1 Data Protection by Design & Default

Controllers are required to put in place appropriate technical and organizational measures (e.g. pseudonymization) which are designed to implement data protection principles, and to integrate safeguards for the protection of data subjects' right ("Privacy by Design"); and ensure that, by default, only personal data necessary for the specific purpose of the processing are processed ("Privacy by Default"). (Art.25, GDPR).

1.8.2 Data Protection Impact Assessment (DPIA)

A DPIA is an assessment through which organizations identify and mitigate risks to individuals arising out of a data processing activity. The GDPR requires organizations to carry out a DPIA before commencing any "high risk" processing activity, e.g. systematic and extensive processing activities (e.g. profiling) and where decisions have legal/significant effects on individuals' large scale, systematic monitoring of public areas through CCTV. If such risks cannot be mitigated and remain high, the controller should consult the DPA prior to the processing. (Art.35-36, GDPR). DPAs have issued their own lists of activities requiring DPIAs in each member state.

1.8.3 Record of Processing Activities

Controllers are required to maintain a record of processing activities which includes mandatory information, e.g. type of data processed, purposes, etc. Processors are also required to keep a record of all categories of processing activities carried out on behalf of the controllers. Whilst the GDPR stipulates that organizations with less than 250 employees could be exempted, such exemption would not be applied if the data processing involves criminal convictions or special categories of personal data. (Art.30, GDPR).

1.8.4 Data Protection Officer ("DPO") and GDPR Representative

The GDPR requires organizations to appoint a DPO if their core activities consist of large-scale processing of special categories of personal data or of data relating to criminal offences or regular and systematic monitoring of individuals on a large scale. A DPO must have sufficient expertise, be independent, and have adequate support and resources. If the DPO fulfils other tasks, she or he must be free from conflicts of interest. The DPO appointment must be publicized generally and to the DPA. The role of the DPO is to inform/advise, monitor compliance and be a single contact point with the organization. (Art.37-39, GDPR).

Additionally, organizations that are based outside the EEA but are subject to the GDPR pursuant to the targeting/ monitoring criterion are required to appoint an EEA-based "GDPR Representative". The GDPR Representative acts as a point of contact in the EEA, handling requests from the data subjects and DPAs as well as helping maintain the record of data processing. (Art.27, 30, GDPR).

1.9 Security and Data Breach Notification

The GDPR defines a personal data breach as "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". In case of a personal data breach, the controller shall without undue delay (where feasible, not later than 72 hours) after having

become aware of it, notify the personal data breach to the competent DPA, unless the breach is "unlikely" to pose a risk to data subjects; where the breach is likely to result in a high risk to the rights and freedoms of data subjects, the controller must notify them. The processor must report to the controller without undue delay after becoming aware of a personal data breach. Moreover, GDPR requires that data controllers must maintain an internal breach register. (Art.33-34, GDPR)

1.10 Cross-border Data Transfer

Please refer to the Part IV - Legal Framework for Cross-border Data flow, the EU section.

1.11 Enforcement

The GDPR established a two-tier administrative fines system. For certain violations, organizations can be fined by competent DPA up to €10 million or 2% of their global annual turnover, whichever is higher; for the most significant infringements of the GDPR, regulators can impose fines of up to €20 million or 4% of an organization's global annual turnover, whichever is higher. In some member states, breaches of data protection legislation can also lead to criminal sanctions.

In addition, individuals have the rights to lodge a complaint with competent DPAs, to seek effective judicial remedy, and to receive compensation from a relevant controller or processor for material or immaterial damage resulting from infringement of the GDPR.

2. United Kingdom

2.1 Overview

2.1.1 Legal System

At the date of writing, the GDPR is directly applicable in the UK, as though it were still an EU member state. In the UK, the Data Protection Act 2018 ("DPA 2018") has been introduced to replace the Data Protection Act 1998 and to supplement the GDPR with UK specific provisions – for example, relating to the processing of special category data and to introduce exemptions for matters such as freedom of expression. In addition, the DPA 2018 contains additional provisions to implement the Law Enforcement Directive; covers processing of personal data by intelligence services; and covers processing of personal data which is out of scope of EU law.

Brexit Note: Although the UK left the EU on 31 January 2020, the GDPR continues to apply directly in the UK until the end of the transition period (31 December 2020). After the transition period, the European Union (Withdrawal) Act 2018 provides that GDPR will be written into UK law and known as the "UK GDPR". Certain consequential amendments will be made to the GDPR and to the DPA 2018 – for example to remove references to the European Commission.

a) Supervisory Authorities

The Information Commissioner is the independent supervisory body for data protection. The Information Commissioner has an Office to support her (the Information Commissioner's Office ("ICO").

Unusually, the ICO has a requirement that controllers, which are established in the United Kingdom, must pay an annual fee to register that they are processing personal data. There are some exemptions to this requirement. More detail is available here.

b) Material and Territorial Scope

The UK GDPR takes a similar approach to territorial scope as the GDPR: it has an establishment criterion and a targeting or monitoring criterion. The targeting/ monitoring criterion applies to organizations which do not have an establishment in the United Kingdom.

c) Data Processing Principles

N/A.

d) Lawful Basis for Processing

Additional derogations that allow for the processing of special categories of personal data and criminal conviction data were introduced in the DPA 2018. There are 16 pages of derogations, which allow processing of special category data for purposes such as research, prevention, and detection of fraud, and for employment law purposes. In order to rely on most of the derogations, the controller must adopt a supplemental "appropriate policy document" which sets out how the controller will comply with principles of the GDPR and retention and erasure. Additional information about the processing of special category data must also be included in the record of processing activities.

2.2 Key Definitions

N/A.

2.3 Data Subject Rights

The DPA 2018 maintains special provisions for credit reference agencies, requiring them to provide access to credit files. It also introduces derogations from individual rights (for example, if fulfilling an access request would tip someone off about an investigation, so prejudicing the prevention and detection of crime) and introduces special procedures for access requests involving health social work and education records.

2.4 Privacy Notice

N/A.

2.5 Direct Marketing

The Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR") (as amended) is the UK implementation of the EU e-Privacy Directive. The ICO issued the draft direct marketing code of practice in January 2020. There can be personal liability for company management if the direct marketing rules under the PECR are breached due to the consent, connivance, or neglect of management.

2.6 Data Sharing and Processing

N/A.

2.7 Children's Privacy Protection

In the UK, the protections for information society services offered to children, on the basis of consent, apply to children who are under the age of 13.

In January 2020, the ICO published a draft code of practice on standards of age-appropriate design for information society services likely to be accessed by children. The code is currently subject to the Parliamentary approval. This has a wide scope and applies to online services likely to be accessed by children under 18.

2.8 Accountability

a) Data Protection by Design & Default

N/A.

b) Data Protection Impact Assessment (DPIA)

N/A.

c) Record of Processing Activities

If special category data is processed in reliance on a derogation in the DPA 2018, there is usually a requirement to include additional information about this in the record of processing activities. See Section 1.8.3 above.

d) Data Protection Officer ("DPO") and GDPR Representative

Brexit Note on the GDPR Representative: After Brexit, organizations which are subject to the UK GDPR on the basis of the targeting/ monitoring criterion, but which are established outside the UK, must appoint a UK representative.

2.9 Security and Data Breach Notification

N/A.

2.10 Cross-border Data Transfer

Brexit Note: Unless the EU Commission grants an adequacy decision, the UK will become a third country at the end of the Brexit transition period which will require alternative safeguards such as SCCs to be put in place to address data transfers from the EEA to the UK. In terms of transfers from the UK at the end of the Brexit transition period, the UK has adopted secondary legislation which confirms that transfers to the EEA will be regarded as made with adequate protection. This is on a provisional basis, so it could be changed. This legislation also confirms that UK based establishments can continue to rely on the SCCs and can continue to transfer personal data to countries determined by the EU to be adequate. Again, this is expressed to be on a provisional basis, so could be changed if the UK decides to

take a different approach to data transfers in future.

2.11 Enforcement

The DPA 2018 also creates certain criminal offences (i.e. deleting personal data in order to avoid providing it in response to an access or portability request, to knowingly or recklessly obtaining or disclosing personal data without the consent of the controller, obstructing the exercise of a warrant by the ICO, etc.) and the responsible director's liability for an offence committed by an organization.

环球律师事务所 GLOBAL LAW OFFICE SINCE 1979

3. Germany

3.1 Overview

3.1.1 Legal System

The German Data Protection Amendment Act which implemented the new German Federal Data Protection Act ("FDPA") was passed on 5 July 2017 and entered into force on 25 May 2018. In this Act, the German legislator has made extensive use of the opening clauses set out in the GDPR and introduced a number of provisions to supplement it – for example, relating to the processing of special categories of data and rules relevant in connection with a designation of a data protection officer. In addition, the FDPA contains provisions to implement the Law Enforcement Directive.

At the federal level, the Second German Data Protection Amendment and Implementation Act dated 20 November 2019 adapted more than 150 federal laws (including i.e. the Freedom of Information Act, eGovernment Act, BSI-Act, Social Security Codes, etc.) to the GDPR requirements. The Federal States have also updated their laws.

3.1.2 Supervisory Authorities

The federal system of Germany (federation of 16 states) affects the supervision of data protection. Data protection supervision comes under the responsibility of the states. However, there is one exception: the telecommunications and postal services companies. Those companies are monitored by the federal government which has assigned that task to the Federal Data Protection Commissioner. In most states, the supervision is exercised by the Data Protection Commissioners. A company is supervised by the authority that has jurisdiction over the district where the company has its headquarters.

3.1.3 Material and Territorial Scope

The FDPA applies to private bodies if

i. the controller or processor processes personal data in Germany,

ii. personal data is processed in the context of the activities of an establishment of the controller or processor in Germany, or if,

iii. although the controller or processor has no establishment in the EU or another contracting state of the EEA, it does fall within the scope of the GDPR, i.e. offers goods or services to individuals in Germany or monitors the behavior of individuals in Germany.

3.1.4 Data Processing Principles

N/A.

3.1.5 Lawful basis for processing

The German legislator has made extensive use of opening clauses and introduced a number of provisions that allow for the processing of special categories of personal data and employee data, including inter alia:

The processing of employee data is generally allowed if necessary for establishing or carrying out the employment relationship. The FDPA also provides clarification on consent in an employer-employment relationship.

The FDPA further permits the processing of sensitive data if the processing is necessary for the purpose of, for example, preventive 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 and services or pursuant to the data subject's contract with a health professional and if these data is processed by health professionals or other persons subject to the obligation of professional secrecy or under their supervision. These further justifications play an important role in practice for companies that are active in the healthcare sector. However, such processing is only possible if safeguards are taken to protect such data.

The FDPA also permits processing of sensitive data without consent for scientific or historical research and for statistical purposes, if the processing is necessary for these purposes and the data controller's interest to process that data significantly outweighs the data subject's interest in not processing the data. To safeguard the interests of the data subject, the data controller must apply "appropriate and specific measures".

In addition, the FDPA contains provisions on scoring, credit checks and consumer loans - these provisions form a basis of the German credit system.

3.2 Key Definitions

N/A.

3.3 Data Subject Rights

The FDPA introduces derogations from individual rights, including in particular:

• The obligation to provide information to the individual: in certain limited cases, where

the controller intends to further process the personal data for a purpose other than that for which the personal data was collected, the FDPA exempts the controller from its obligation to inform the individual of their rights. This is, for example, the case if providing information about the planned further use would interfere with the establishment, exercise, or defense of legal claims (provided that there is no overriding interest of the individual in the provision of the information).

- The right to access data: in the context of scientific research, there is an exception in relation to the right of access if the data is necessary for purposes of scientific research and the provision of information would involve disproportionate effort. In addition, the FDPA contains certain exemptions from the data subject's right to access data if, for example, such data was recorded only because they may not be erased due to legal or statutory provisions on retention, or only serve purposes of monitoring data protection or safeguarding data, and providing information would require a disproportionate effort, and appropriate technical and organizational measures make processing for other purposes impossible.

- The right to erasure: the FDPA exempts the controller from its obligation to erase personal data where the erasure, in case of non-automatic data processing, would be impossible, or would involve a disproportionately high effort due to the specific mode of storage and the data subject has a minor interest for erasure. In this case, restriction of processing applies, however, in place of erasure.

3.4 Privacy Policy

N/A.

3.5 Direct Marketing

The direct marketing rules set out in the Act against Unfair Competition (Gesetz gegen den unlauteren Wettbewerb, UWG) is the German implementation of the EU e-Privacy Directive. These rules contain specific restrictions the companies need to comply with when conducting certain kinds of direct marketing (in particular promotional electronic communications). These rules apply even if no personal data is involved (e.g. if sending out marketing communications to generic email accounts like info@company.com). These rules will be replaced by the proposed Regulation on Privacy and Electronic Communications in due course.

3.6 Data Sharing and Processing

N/A.

3.7 Children's Privacy Protection

Germany has not made use of an opening clause providing for the possibility to deviate from the age of 16 as an age limit with respect to the processing of a child's personal data in relation to information society services.

3.8 Accountability

a) Data Protection by Design & Default

N/A.

b) Data Protection Impact Assessment (DPIA)

N/A.

c) Record of Processing Activities

N/A.

d) Data Protection Officer (DPO) and GDPR Representative

The threshold for the appointment of a DPO is much lower in Germany than compared to that of the GDPR. In addition to the GDPR requirements, the controller and processor must designate a DPO when (i) they constantly employ as a rule at least 20 persons dealing with the automated processing of personal data; or, regardless of the number of persons involved in the processing of personal data, (ii) whenever a DPIA has to be carried out; or (iii) whenever personal data is processed to be transferred for commercial reasons, transferred anonymously or for purposes of market research and opinion polls.

3.9 Security and Data Breach Notification

N/A.

3.10 Cross-border Data Transfer

N/A.

3.11 Enforcement

The FDPA creates certain criminal offences which foresee imprisonment or fine for:

- deliberate and not authorized transfer / making accessible non-publicly available personal data of a large number of individuals for commercial purposes;

- not authorized processing of non-publicly available personal data in return for payment or for personal or third-party enrichment purposes or with the intention of harming another person;

- fraudulent obtainment of non-publicly available personal data in return for payment or for personal or third-party enrichment purposes or with the intention of harming another person.

In addition, in connection with consumer loans, the FDPA sets out administrative fines for failure to handle a data subject access request appropriately or to inform a consumer or to inform them fully and correctly within the prescribed time limits.

环球律师事务所 GLOBAL LAW OFFICE SINCE 1979

4. France

4.1 Overview

4.1.1 Legal System

In addition to the GDPR which is directly effective in France, the French legal framework on data protection is set out by the "Loi Informatique et Libertés" (the French Data Protection Act) no. 78-17 of 6 January 1978 and its implementing decree. The French Data Protection Act was amended for the last time by the law 20 of June 2018 in order to:

ensure proper articulation between with France specific provisions and GDPR provisions, and

transpose the Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

The main provisions of the law of 20 June 2018 retroactively entered into force on 25 May 2018, which was the date of entry into force of the GDPR.

The decree no. 2005-1309 of 20 October 2005 implementing the French Data Protection Act was also amended by a decree of 1st August 2018 (the "Decree").

4.1.2 Supervisory Authorities

The Commission Nationale de l'Informatique et des Libertés ("CNIL") is the independent supervisory authority for data protection in France. The authority was created by the 1978 law.

In France, there is no requirement for controllers to pay an annual fee to register that they are processing personal data. The 2018 law abolished the prior declaration and authorization regimes. Prior authorization requirements have been maintained to a very limited extent in case of processing of health data (Chapter IX, article 54, III).

4.1.3 Material and Territorial Scope

The territorial scope of the French Data Protection Act slightly differs from the GDPR. It applies to the processing of personal data where the controller or the processor is established on the French territory (no matter if the processing is carried out in France or not)

In addition, the provisions of the French Data Protection Act which concern the areas where

the GDPR allows Member States to legislatively as soon as the data subject is a French resident (no matter if the controller is not established in France).

4.1.4 Data Processing Principles

N/A.

4.1.5 Lawful basis for processing

Additional derogations that allow for the processing of special categories of personal data were introduced in the French Data Protection Act. These derogations notably cover:

- processing carried out by employers or administrations relating to biometric data strictly necessary for controlling access to workplace as well as to devices and applications;
- processing relating to the reuse of public information appearing in judgments and decisions provided that such processing has neither the purpose nor the effect of allowing the re-identification of the persons concerned;

Processing necessary for public research after a reasoned and published opinion from the CNIL.

4.2 Key Definitions

N/A.

4.3 Data Subject Rights

The French Data Protection Act provides additional data protection rights. It provides data subjects a right to set down instructions for the management of their personal data post mortem. It also provides minors with a specific right of erasure as further detailed below. Data controllers are required to inform data subjects about the existence of these rights.

4.4 Privacy Policy

N/A.

4.5 Direct Marketing

The French rules on direct marketing by way of electronic communications are derived from the European directive 2002/58/EC on privacy and electronic communications ("ePrivacy directive"). They have been introduced into the French Post and Electronic Communications

Code (“PECC”) by the 2004 French Act on the Confidence in the Digital Economy (“LCEN”).

Pursuant to article L. 34-5 of the PECC, “is prohibited the use of automated electronic communication systems, facsimile machines (fax) or email using the contact details of an individual, subscriber or user, who has not given its prior consent to receive direct marketing through this mean”. The notion of “direct marketing” is very broad and covers any message intended to promote, directly or indirectly, the goods, the services or the image of a person selling goods or services.

4.6 Data Sharing and Processing

N/A.

4.7 Children’s Privacy Protection

In France, the protection for information society services offered to children, on the basis of consent, apply to children who are under the age of 15.

The French Data Protection Act provides minors a specific right to be forgotten. Upon data subject request, data controllers are required to erase as soon as possible personal data collected when data subject was a minor via provision of information society services. If the data controller has communicated the personal data to a third-party controller, it shall take reasonable measures to inform this third party that the person concerned has asked for the erasure of all links towards this data as well as any copy or reproduction.

In the event of refusal to respond or of absence of response from the data controller to the person within one month of the request, the person may take the matter to CNIL which shall rule on the matter within 3 weeks.

4.8 Accountability

a) Data Protection by Design & Default

N/A.

b) Data Protection Impact Assessment (DPIA)

N/A.

c) Record of Processing Activities

N/A

d) Data Protection Officer (DPO) and GDPR Representative

N/A

4.9 Security and Data Breach Notification

N/A.

4.10 Cross-border Data Transfer

N/A

4.11 Enforcement

Breaches of certain provisions of the French Data Protection Act and the GDPR are also subject to criminal penalties in France. Examples of breaches are violations of the security requirement, unlawful collection of personal, breach of the limited retention principle, etc.

5. Netherlands

5.1 Overview

5.1.1 Legal System

At the date of writing, the GDPR is directly applicable in the Netherlands. In addition to that, the Dutch Implementing Act GDPR (Uitvoeringswet AVG, UAVG) was introduced in 2018 to replace the Dutch Data Protection Act (Wet Bescherming Persoonsgegevens) and to supplement the GDPR with Dutch specific provisions – for example, relating to the processing of special category data, formalizing the supervisory authority and to introduce exemptions for matters such as freedom of expression.

5.1.2 Supervisory Authorities

The Autoriteit Persoonsgegevens (AP) is the independent supervisory body for data protection and is established through various provisions in the UAVG. While the AP also covers the processing of personal data through email marketing, cookies, and similar technologies, it must be noted that rules around spam and cookies are enshrined in the Dutch Telecommunications Act (Telecommunicatiewet, Tw) and primarily supervised by the Authority Consumer and Market (Autoriteit Consument en Markt, ACM).

5.1.3 Material and Territorial Scope

The UAVG takes a similar approach to territorial scope as the GDPR: it has an establishment criterion and a targeting or monitoring criterion. The targeting/ monitoring criterion applies to organizations which do not have an establishment in the Netherlands.

5.1.4 Data Processing Principles

N/A.

5.1.5 Lawful basis for processing

Additional derogations that allow for the processing of special categories of personal data and criminal conviction data were introduced in the UAVG. There are 12 articles with derogations, which allow processing of special category data for purposes such as research, prevention, and detection of fraud, and for employment law purposes.

5.2 Key Definitions

N/A.

5.3 Data Subject Rights

The UAVG maintains special provisions for data subject rights in relation to automated decision making and use of personal data in the context of use for academics, journalism, and art. It also introduces derogations from individual rights (for example, if fulfilling an access request would tip someone off about an investigation, so prejudicing the prevention and detection of crime), specific rules in relation to scientific use and exemptions on data breach notification obligations for financial institutions.

5.4 Privacy Policy

N/A.

5.5 Direct Marketing

The Dutch Telecommunications Act or Tw as mentioned earlier above is the Dutch implementation of the EU e-Privacy Directive. Relevant provisions around unsolicited electronic communications and cookies are primarily supervised by the ACM, with further supervision from the AP insofar it relates to the processing of personal data. In recent years, the AP has been increasingly active in the field of direct marketing, producing guidance on spam and cookies and actively supervising in these areas, while ACM seems to have taken a step back. It must be noted that in specific cases (as proven by the ACM in the past), there can be personal liability for company management if the direct marketing rules under the Tw are breached.

5.6 Data Sharing and Processing

N/A.

5.7 Children's Privacy Protection

In the Netherlands, the protections for information society services offered to children, on the basis of consent, apply to children who are under the age of 16.

5.8 Accountability

a) Data Protection by Design & Default

N/A.

b) Data Protection Impact Assessment (DPIA)

N/A.

c) Record of Processing Activities

N/A.

d) Data Protection Officer (DPO) and GDPR Representative

N/A.

5.9 Security and Data Breach Notification

N/A.

5.10 Cross-border Data Transfer

N/A.

5.11 Enforcement

N/A.

6. Spain

6.1 Overview

6.1.1 Legal System

The GDPR is directly applicable in Spain. In addition to it:

- The Organic Law 3/2018, of 5 December, on the Protection of Personal Data and granting the digital rights (the "Spanish Data Protection Act") supplements and/or completes some of the GDPR provisions; and

- The Law 34/2002, of 11 July, on Information Society Services and e-Commerce includes provisions on direct marketing and cookie requirements (the "ISS Law").

Further to the above, the Spanish Data Protection Authority's (the "AEPD") guidance and recommendations are also relevant for the purposes of interpreting data protection obligations.

6.1.2 Supervisory Authorities

The AEPD is the independent supervisory body for data protection in Spain. Further to the AEPD, there are two regional supervisory authorities (Catalonian and Basque data protection authorities) that are competent with regards to processing activities carried out by regional public authorities or by private entities carrying out a public regional function.

6.1.3 Material and Territorial Scope

The Spanish Data Protection Act takes a similar approach to material scope as the GDPR but does not provide for its own territorial scope of application, although it is generally interpreted that the establishment and targeting or monitoring criterion would similarly be applicable.

6.1.4 Data Processing Principles

The Spanish Data Protection Act establishes a specific obligation related to the data retention principle. Before fully erasing personal data (either because it is no longer necessary for the purposes pursued or because the data subject has exercised an erasure request) it shall be kept duly blocked for an additional period of time during which legal claims may be exercised. By duly blocked, the Spanish Data Protection Act means storing the information in a way that the personal data is not accessible by anyone unless it is requested by competent public authorities or for the exercise or defense of legal claims. Blocked data cannot be

processed for any purpose other than the indicated above. Only once the blocking period elapses, the personal data can be fully destroyed.

6.1.5 Lawful basis for processing

Certain specificities regarding the processing of some special categories of personal data and criminal conviction data were introduced in the Spanish Data Protection Act. In short:

- The data subject's consent is not enough in order to process certain special categories of personal data concerning him unless it is necessary for a clear and lawful purpose. This means that "when the main purpose (of processing this data) is merely identifying the ideology, trade union membership, sexual orientation, beliefs or racial or ethnic origin" of the data subject, consent of the affected individual will not be enough to process this data. The purpose of this provision is avoiding discriminatory situations (e.g. preventing that, for example, an individual is not hired because of his/her racial origin).

- The processing of this criminal data is highly restricted in Spain. This information can only be processed for the prevention, investigation, detection of potential criminal offences or in order to judge whether a criminal offence has been committed. This entails that the processing of this information is mostly restricted to competent authorities and law enforcement bodies. Also, lawyers and barristers are entitled to process this data with the purpose of providing a service to their clients. In any other case, this information can only be processed if it is established in an applicable law.

6.2 Key Definitions

N/A.

6.3 Data Subject Rights

N/A.

6.4 Privacy Policy

N/A.

6.5 Direct Marketing

The ISS Law is the law that gathers most of the provisions that are the consequence of the implementation of the EU e-Privacy Directive in Spain. This law includes the requirements that need to be met in order to send direct marketing through electronic means.

6.6 Data Sharing and Processing

N/A.

6.7 Children's Privacy Protection

In Spain, the processing of children's personal data upon their consent is only possible if they are over 14 years old.

6.8 Accountability

a) Data Protection by Design & Default

N/A.

b) Data Protection Impact Assessment (DPIA)

N/A.

c) Record of Processing Activities

N/A.

d) Data Protection Officer (DPO) and GDPR Representative

The Spanish Data Protection Act states that controllers and processors shall appoint a DPO as provided by Article 37(1) of the GDPR but, as an example, includes a list of industries that are likely to fall within the scope of said article. It needs to be noted that such list is not exhaustive, as the AEPD has confirmed (i.e. it is only provided as a set of examples). Below is the list of said industries:

- official associations of professionals and general councils of professionals;
- educational centers offering regulated studies as provided by the Spanish Right to Education Act and public and private universities;
- entities operating electronic communications networks and offering electronic communication services, as stated by the General Telecommunications Law, processing personal data on a large scale;
- information society services providers carrying out data subjects' profiling activities on a large scale;

- banks, credit unions and the Official Credit Institute;
- private financial credit institutions;
- insurance and reinsurance companies;
- investment services companies subject to the stock market legislation;
- energy and natural gas distributors and marketers;
- entities in charge of creditworthiness data files and in charge of fraud prevention data files;
- entities carrying out advertising and commercial research activities based on the data subjects' preferences or carrying out data subjects' profiling activities;
- health facilities legally obliged to keep patients' medical histories (health professionals acting on their own as freelances are excluded);
- entities carrying out business/credit reports regarding individuals;
- entities offering gambling and gaming services by electronic, informatics, telematics, or interactive means;
- private security companies; and
- sports federations when processing underage individuals' personal data.

No specific provisions exist concerning the appointment of GDPR representatives.

6.9 Security and Data Breach Notification

N/A.

6.10 Cross-border Data Transfer

N/A.

6.11 Enforcement

N/A.

II. North America

1. United States

1.1 Overview

1.1.1 Legal System

At the federal level, there is no single all-encompassing and comprehensive Data Protection or Privacy Law in the United States. Instead, there are a number of sector-specific laws that vary considerably in their purpose and scope. For example, The Gramm-Leach-Bliley Act (GLBA) imposes data protection obligations on financial institutions in protecting "consumer non-public personal information "; The Health Insurance Portability and Accountability Act (HIPAA) applies to "covered entities" relating to the provision of health care in protecting "protected health information"; The Electronic Communications Privacy Act of 1986 （ECPA） protects wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers. The Act applies to email, telephone conversations, and data stored electronically and provides for criminal and private civil liability for violations of its provisions. Notably, U.S. attaches a big importance to children' privacy and promulgated COPPA, which specify the basic principles and requirements of protection at the federal level. The cornerstone COPPA provides a clear guidance to each state.

Horizontally, state efforts to pass comprehensive privacy laws are gaining momentum. All 50 states have proposed bills and the majority have yet to pass the legislative process. Currently, three states (California, Nevada, and Maine) have passed their own privacy bills and the landmark California Consumer Privacy Act (CCPA), which became effective on January 1 2020 is by far the most comprehensive legislation in the States. To govern compliance with the CCPA, on August 14, 2020, the Office of Administrative Law approved with immediate effect the Department of Justice's CCPA regulations (CCPAR). The regulations establish procedures for compliance and exercise of rights, as well as clarifying important transparency and accountability mechanisms for businesses subject to the law. Violations of these regulations will constitute a violation of the CCPA and be subject to the remedies set out in the CCPA.

1.1.2 Supervisory Authorities

Though the U.S. has no plenary data protection regulator to date, the customer protection authorities, e.g. the Federal Trade Commission (FTC), are empowered to bring enforcement actions against violations of consumer privacy and require companies to take steps to remediate the unlawful behavior. This legal authority primarily comes from Section 5 of The Federal Trade Commission Act, which prohibits unfair, deceptive, or fraudulent practices in

the market place. A company's failure to comply with established privacy policies or codes constitute deceptive practice. In addition, FTC is a major authority that enforces a variety of privacy laws including but not limited to above-mentioned GLBA, FCRA and Children's Online Privacy Protection Act (COPPA). Other customer protection authorities (such as Federal Communications Commission) are also entitled to enforce the data protection.

With regards to state laws like CCPA, Attorney Generals for the relevant state can be the competent authority.

1.1.3 Material and Territorial Scope

Activities of companies in other countries impacting the privacy and data rights of U.S. citizens may fall under the jurisdiction of U.S. laws.

For example, the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) passed in March 2018., allowing federal law enforcement to compel U.S.-based technology companies via warrant or subpoena to provide requested data stored on servers regardless of whether the data are stored in the U.S. or on foreign soil. The U.S. Department of Justice explicitly states that a foreign company located outside the United States providing services in the United States who has sufficient contacts in the U.S. may be subject to U.S. jurisdiction depending on the nature, quality, and quantity of the contact.[6]

In the absence of a general data protection law, this section will mainly introduce the material and territorial scope of CCPA.

The CCPA only applies to business that meet any of the following criteria:

1) Has gross annual revenues in excess of $25 million;

2) Buys, receives, or sells the personal information of 50,000 or more Californian consumers, households, or devices;

3) Derives 50 percent or more of annual revenues from selling consumers' personal information.

Businesses under the CCPA are required to:

1. Inform consumers as to the categories of personal information to be collected and the purposes for which it is used;

2. Delete a consumer's personal information upon request;

6 U.S. Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act White Paper, April 2019, p 8

3. Disclose to a consumer specific information about the personal information it has collected;

4. Disclose to a consumer whether personal information is sold or otherwise shared and to whom;

5. Comply with a consumer's request that personal information not be sold to third parties;

6. Obtain affirmative authorization before selling the personal information of a consumer under the age of 16;

7. Refrain from discriminating against consumers who exercise their rights under the statute.

1.1.4 Data Processing Principles

Although few U.S. privacy acts clearly sets out data processing principles, the FTC has recognized some common principles in its Recommendations named Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policy Makers (FTC Recommendations).

Data Security - Companies should provide reasonable security for consumer data.

Limitation Collection - Companies should limit data collection to that which is consistent with the context of a particular transaction or the consumer's relationship with the business, or as required or specifically authorized by law.

Collection Limitation - Companies should implement reasonable restrictions on the retention of data and should dispose of it once the data has outlived the legitimate purpose for which it was collected. Retention periods, however, can be flexible and scaled according to the type of relationship and use of the data

Data Accuracy - Companies should maintain reasonable accuracy of consumers' data but the approach to improving accuracy is flexible, scaled to the intended use and sensitivity of the information.

Transparency - Companies should increase the transparency of their data practices.

(i) Privacy notices should be clearer, shorter, and more standardized to enable better comprehension and comparison of privacy practices.

(ii) Companies should provide reasonable access to the consumer data they maintain; the extent of access should be proportionate to the sensitivity of the data and the nature of its use.

(iii) All stakeholders should expand their efforts to educate consumers about commercial data privacy practices.

1.1.5 Lawful basis for processing

While this requirement is not directly stipulated, it is commonly acknowledged that a prior notice shall be provided and information shall be disclosed about the collection, use, retention or sell of personal information at the request of a consumer.

In limited circumstances where sensitive data is collected or where the use of personal data is materially different than claimed, companies should obtain affirmative express consent.

1.2 Key Definitions

Consumer - The CCPA defines consumer to mean "a natural person who is a California resident under the California Code of Regulations. The Act applies to every California resident, whether or not they are a customer of the covered business. Accordingly, employees of a business or a business's vendors could be consumers.

Personal Information - The definition is not uniform across all states or regulations. Considering that CCPA is the most comprehensive privacy law in effect, this Guide will reference the CCPA definition.

Under CCPA, "Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a consumer or household. CCPA lists the types of personal information and provides corresponding examples to explain the data that may or may not fall into the scope of personal information.

Household: The CCPAR defines "Household" to mean a person or group of people who:

(1) reside at the same address;

(2) share a common device or the same service provided by a business; and

(3) are identified by the business as sharing the same group account or unique identifier.

Sensitive Personal Information - This concept is not present in many current U.S. privacy legislation and its scope varies widely by sector and state. California has always been a front runner in U.S. privacy law making and has introduced the concept of "sensitive personal information" to the proposed California Privacy Rights and Enforcement Act 2020 (CPRA).

Under the CPRA, "Sensitive personal information" means; a consumer's social security number, driver's license, state identification card, or passport number; a consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; a consumer's precise geolocation; personal information revealing a consumer's racial or ethnic origin, religion, or union membership; the contents of a consumer's private communications, unless the business is the intended recipient of the communication; a consumer's biometric information; data concerning to consumer's health; data concerning a consumer's sexual orientation; or other data collected and analyzed for the purpose of identifying such information.

It should be noted that some of the data fields in the CPRA are also included in the list of 14 data types in the CCPA which if breached (in conjunction with the consumer's name) as a result of a failure to implement reasonable security, a Consumer is allowed to bring a suit.

FTC takes the position that defining what constitutes sensitive data is a complex task and often depend on context[7]. Despite the complexity, FTC recognized some clear examples of sensitive data, including children's information and those stipulated in CPERA.

Data Controller-This term is not used in the CCPA. However, the Washington Privacy Act recognizes the role of controller and define it as the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor-This term is not used in the CCPA. Nonetheless, Washington Privacy Act recognizes the role of a processor and defines it as a natural or legal person who processes personal data on behalf of controller.

Third Party-The CCPAR defines "Categories of third parties" to mean types or groupings of third parties with whom the business shares personal information, described with enough particularity to provide consumers with a meaningful understanding of the type of third party. They may include advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers.

1.3 Data Subject Rights

Data subject rights are statute-specific and this section will mainly talk about what rights CCPA grants Consumers. Under the CCPA a consumer shall have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected. The scope and type of information that is subject to this right is defined in the CCPA. The business must

7 FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising, p 55.

promptly take steps to disclose and deliver, free of charge to the consumer, the personal information requested upon receipt of a verifiable consumer request.

Right to be Informed - The right of Consumers to know what personal information is being collected about them and whether their personal information is sold or disclosed and to whom. A business may provide personal information to a consumer at any time, but shall not be required to provide personal information to a consumer more than twice in a 12-month period. The CCPA provides further details on the methods and format for delivering such information.

Right to Opt-Out - The right of Consumers to say no to the sale of personal information.

Right of Access - The right of Consumers to request a business to disclose and deliver the categories and specific pieces of their personal information that the business has collected.

Right of Non-Discrimination - The right of Consumers to equal service and price, even if they exercise their privacy rights.

Right to Delete - The right of Consumers to request deletion of any personal information collected. While a business that receives a verifiable request from a consumer to delete the consumer's personal information shall delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records. Article 3 of the CCPAR provides further details on complying with requests to delete. It covers the methods for submitting such requests.

Right of Portability - The right of Consumers to receive information in a portable and, to the extent technically feasible, readily useable format.

In addition to these rights, consumers may be entitled under other privacy laws to the right to rectification, right to restrict processing, right to object, right against automated decision-making and right of complaint/ private action.

Right to Verify - The CCPAR provides two methods businesses can use to verify the identities of individuals submitting data access and deletion requests. First, if a business maintains a password-protected account, it "may verify the consumer's identity through the business's existing authentication practices for the consumer's account," provided this complies with other CCPA requirements. Second, if the individual does not have a password-protected account, identity verification becomes more complex and is subject to different standards, depending on the nature of the request and the type of the personal information at issue.

The CCPAR also details how to respond to such requests and the timelines to comply with when confirm and responding to such requests. In responding to requests to know, the CCPAR

also sets out certain conditions which must all be met before a business is not required to search for personal information. It also specifies the type of information that must not be disclosed when such a request is made. For example. financial account number, any health insurance or medical identification number, an account password, security questions and answers, or unique biometric data.

1.4 Privacy Policy

Since there's no federal data protection law, this section will focus on requirements of California.

California Online Privacy Protection Act (CalOPPA) requires the operators (i.e., owners) of commercial websites or online services that collect personally identifiable information (PII) of California residents through the Internet to conspicuously post a privacy policy on their site or service. Cal. Bus. & Prof. Code § 22575(a).

To comply with CalOPPA, a privacy policy must: Identify the categories of PII collected through the website or online service and the categories of third parties with whom the PII may be shared;

1. Describe the process (if any) through which consumers may review and request changes to their PII;

2. Describe the process by which the operator notifies consumers of material changes to the privacy policy;

3. Clearly state the effective date of the policy;

4. Disclose how the operator responds to Web browser Do Not Track (DNT) signals or similar mechanisms, if the operator collects PII across third-party websites or online services;

5. Disclose whether third parties may collect PII when a consumer uses the operator's website or online service.

With regard to the requirement to conspicuously post the privacy policy, Cal. Bus. & Prof. Code 22577(b) set out requirements on the use of icons, text links, hyperlinks and covers positioning of the policy on websites and accessibility to the policy on mobile apps.

• **To comply with the CCPA:**

Business must disclose the following information in its online privacy policy and update that information at least once every 12 months:

(1) A description of a consumer's rights under CCPA;

(2) A list of the categories of personal information it has collected about consumers in the preceding 12 months;

(3) A separate link to the "Do Not Sell My Personal Information".

• **The CCPAR gives further guidance on privacy policies. For example:**

(1) How to design and position of policies so that they are easy to read and understandable to consumers;

(2) How to ensure that the policy is reasonably accessible to consumers with disabilities;

(3) Information which must be included in the privacy policy;

(4) Instructions on the Right to Request Deletion of Personal Information;

(5) Instructions on the Right to Opt-Out of the Sale of Personal Information;

(6) Instructions on the Right to Non-Discrimination for the Exercise of a Consumer's Privacy Rights.

1.5 Direct Marketing

U.S. extensively regulates direct marketing communications.

Email - The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act) sets rules for commercial email messages. Companies must include a clear and conspicuous explanation of how the recipient can opt out and honor opt-out requests promptly.

Text Message - Automated marketing or promotional messages requires express written consent under Telephone Consumer Protection Act (TCPA).

Telemarketing - On the national level, Telemarketing and Consumer Fraud and Abuse Prevention Act prohibits telemarketers from engaging in a pattern of unsolicited telephone calls that a reasonable consumer would consider an invasion of privacy. Different bills impose calling time restrictions, do-not-call registries, opt-out requests, mandatory disclosures, restrictions on the use of auto-dialers and pre-recorded messages, etc.

1.6 Data Sharing, Processing, and Broking

FTC has not published instructions on data sharing. Yet, the White House published a Guidance on Inter-Agency Sharing of Personal Data Protecting Personal Privacy in 2000 and proposed the requirement of notice, consent, re-disclosure limitation, accuracy, security controls, minimization, accountability, and privacy impact assessments. consumers Although this guidance applies directly only to programs covered by the Computer Matching and Privacy Protection Act and governmental bodies, organizations should consider applying these principles in other data sharing contexts.

There are no specific data sharing articles in CCPA but Consumer have the right to request a business disclose the categories of third parties with whom the business shares personal information.

The CCPA defines a data broker as "a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship." The California law on data brokers requires data brokers covered by the law to register with the Attorney General and to provide certain information on their practices. Consumers will be able to opt-out of the sale of their personal information. However, CCPA's definition of "personal information" does not include information lawfully made available from government records.

1.7 Children's Privacy Protection

U.S. Congress enacted the Children's Online Privacy Protection Act (COPPA) in October 1998 and the FTC accordingly promulgated the Children's Online Privacy Protection Rule (Rule). COPPA and the Rule regulates the collection of personal information from children under 13 by online services including websites, advertising, and mobile apps. The primary goal of COPPA is to place parents in control over what information is collected from their young children online. Principally, operators are required to provide notice directly to parents, obtain verifiable parental consent, allow parents to review personal information collected from their children, allow parents to revoke their consent, and delete information collected from their children at the parents' request.

In addition to the requirements under COPPA, under Article 5. of the CCPAR special rules are set out for consumers under the age of 16 which deal with establishing, documenting, and complying with a reasonable method for determining that the person affirmatively authorizing the sale of the personal information about the child is the parent or guardian of that child. The CCPAR also provides methods to ensure that the person providing consent is the child's parent or guardian. For Consumers between 13 to 15, there are requirements for allowing such consumers to opt-in to the sale of their personal information and also the right and process to opt-out later.

1.8 Accountability

a) Data Protection by Design and by Default

FTC Recommendations set forth the principle of Privacy by Design and state that companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services.

FTC also calls on companies to adopt best practices making privacy the "default setting" for commercial data practices.

b) Data Protection Impact Assessment (DPIA)

FTC Recommendations suggest that companies should maintain comprehensive data management procedures throughout the life cycle of their products and services. One of the management procedures is conducting privacy risk assessments to promote accountability, and help identify and address privacy issues.

In particular, Washington Privacy Act Section 9 sets out that companies must conduct and document a data protection assessment in a number of circumstances including processing of personal data for the purpose of targeted advertising, sale of personal data and processing of sensitive personal data.

c) Record of Processing Activities

Overall, there's no statutory requirement to document or maintain records of processing activities. However, as mentioned above, the state of Washington specifies that companies must document data protection assessment in certain scenarios.

d) Data Protection Officer (DPO) and Representative

With a few exceptions, appointment of a Data Protection Officer is not required under U.S. law. Certain statutes like HIPAA and Massachusetts state law require the appointment or designation of an individual or individuals responsible for compliance with privacy or data security requirements.

1.9 Security and Data Breach Notification

FTC Recommendations states that data security is a fundamental Privacy by Design principle and companies must provide reasonable security for consumer data. Federal and state statutes like GLBA and New York Privacy Act (not passed) require entities to maintain the confidentiality and security of personal information or reasonably secure personal information from unauthorized attacks. Furthermore, the FTC has published a guide for

business regarding data security based on previous cases[8].

Federal laws and states have adopted their own data breach notification rule, for example, HIPAA Breach Notification Rule and California Information Practice Act of 1977. Generally, entities need to provide notification to affected individuals; and competent authorities within a reasonable period.

Californian rule further specifies that the security breach notification shall be written in plain language, covering "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information."

1.10 Cross-Border Data Transfer

There are few express restrictions on storing personal data outside the U.S., but some states have restrictions on data access, maintenance, and processing from outside the U.S. with respect to government contracts and off-shore outsourcing situations.

Notably on July 16 2020, the Court of Justice of the European Union ruled that EU-U. S. Privacy Shield mechanism does not provide data subjects with adequate protection equivalent to EU Law and is therefore invalid. Companies can no longer rely on this approach for data transfers between the U.S. and EEA countries.

1.11 Enforcement

Since taking office in January 2017, Attorney General for California has secured settlements and other novel injunctions covering the full range of violations from improperly exposing the personal information, failing to notify regulators and users of a data breach, failing to provide reasonable data security, failing adequately secure or illegally revealing sensitive information; and illegally preinstalling software that compromised the security of its computers. No specific industry or sector appears to be targeted since the beginning of the enforcement period.

We also recommend that businesses read and understand the nuances of both the statute and the CCPAR because violations of the CCPAR can lead to also penalties.

The two most recent cases prosecuted by California's Attorney General involved personal and medication information and alleged violations of the Unfair Competition Law and Business and Professions Code. Business should therefore be aware of deficiencies in basic data security, including controlling access to computers holding sensitive information, protecting account credentials and passwords from unauthorized use, updating security tools, and adequately logging and monitoring network activity to detect malicious activity. Businesses

8 Available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

should also be careful not to misrepresent the type and level of security provided to consumers.

FTC's enforcement action includes monetary penalties, mandatory implementation of comprehensive privacy and security programs, prohibition to use personal information, provide redress to consumers, deletion of illegally obtained consumer information, etc.

According to the Privacy & Data Security Update Report, FTC brought more than 130 spam and spyware cases and 80 general privacy lawsuits in 2019, including the famous Facebook and Cambridge Analytica case where the tech giant faced an unprecedented 5 billion USD penalty.

1.12 Upcoming Changes to Legislation

Spurred by CCPA, a number of camps including the big tech companies and privacy advocates have been calling for a federal privacy law. Senate bills like Consumer Online Privacy Rights Act, Consumer Data Privacy Act and Data Protection Act propose the creation of a U.S. federal data protection agency with the authority to enforce data practices across the country have been proposed to protect the privacy of Americans.

Until a federal law is in place, it is expected that more individual states would work towards passing their own data privacy laws. Special attention should be paid to New York Privacy Act, Washington Privacy Act and Massachusetts Senate Bill 120.

2.Canada

2.1 Overview

2.1.1 Legal System

The main privacy legislation of Canada is the Federal Personal Information Protection and Electronic Documents Act S.C. 2000, ch. 5 ("PIPEDA"). Alberta, British Columbia and Québec also have their own jurisdictional privacy acts which are substantially similar to PIPEDA. Collectively, the abovementioned legislations constitute the Canadian Privacy Statutes. There are also a number of binding legislations regulating anti-spam[9], radio-television, telecommunication, and electronic documents. Most of the provinces in Canada have separate health privacy legislation protecting health information regarding healthcare services.

2.1.2 Supervisory Authorities

The Office of the Privacy Commissioner of Canada (OPC) oversees and enforces the relevant data protection law. For example, Canada's Anti-Spam Legislation, SC 2010 c 23 ("CASL") is administered by the Canadian Radio-television and Telecommunications Commission, the Competition Bureau Canada and the OPC. Each regulatory authority has jurisdiction over particular aspects of CASL requirements and enforcement.

2.1.3 Material and Territorial Scope

PIPEDA governs the collection, use and disclosure of personal information in the course of commercial activities within its provinces across Canada, not including Alberta, British Columbia and Québec where their own legislations apply. Unlike PIPEDA the statutes for Alberta, British Columbia and Québec apply irrespective of whether an activity is commercial in nature and applies to employee personal information as well. PIPEDA also applies to personal information in connection with the operation of a federal work, undertaking or business, e.g. banks, railways, canals, airlines, and telecommunications companies.

PIPEDA does not have a specific territorial clause. However, according to the Federal Court of Canada, PIPEDA applies to businesses established in other jurisdictions on the basis of 'real and substantial connection' between Canada and the organizations' activities. Factors relevant to the establishment of connections include where promotional efforts are being targeted, the location of end-users, the sources of the content on the website, the location of the website operator and the location of the host server.

9 Canada's Anti-Spam Legislation, SC 2010 c 23 ('CASL'). CASL regulates, among other things, the sending of commercial electronic messages such as promotional and marketing messages, to and from Canada, irrespective of whether the recipient is an individual or an organization. In addition, CASL is an opt-in regime in respect of commercial electronic messages. It prohibits the sending of commercial electronic messages, unless express consent or implied consent, or an applicable exception, is applicable and prescribed requirements are met. Substantial monetary penalties and other consequences can flow from violations of CASL, including extended liability for directors and officers.

2.1.4 Data Processing Principles

PIPEDA contains 10 fair information principles including the principles of accountability, identifying purposes, consent, limiting collection, limiting use, disclosure, retention, accuracy, safeguards, openness, individual access, and challenging compliance. The other provincial statutes set out similar requirements.

2.1.5 Lawful basis for processing – Schedule 1 PEPIDA

An organization may collect, use, or disclose personal information only for appropriate purposes and with the knowledge and consent of data subject. The collection of personal information shall be limited to which is necessary for the purposes identified by the organization and be conducted by fair and lawful means. Consent may be express or implied, depending on the circumstances, the intended collections, uses, and disclosures, and the level of sensitivity of the information. Consent is not required if the collection is clearly in the interests of the individual, consent cannot be obtained in a timely way, and where it is reasonable to expect that the collection with the consent of the individual would compromise the availability of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the Canada's federal or provincial laws. In addition, PIPEDA permits organizations to disclose personal information to another organization under certain situations even where consent is not obtained.

2.2 Key Definitions

a) **Personal Data -** Personal information means information about an identifiable individual. Information is generally considered to fit the definition of "personal information" where there is a serious possibility that an individual could be identified through the use of the information, alone or in combination with other available information.

Sensitive Data - "Sensitive data" is not defined under PIPEDA or provincial data protection statutes. PIPEDA provides that any information can be sensitive depending on the context.

b) **Data Controller and Processor -** Canadian Privacy Statutes do not specifically define data controller or processor. However, the statutes refer to the concept of 'organizations' which includes both data controller and processor.

2.3 Data Subject Rights

• **Access – Article 4.9 Schedule 1 PIPEDA**

Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual shall be

able to challenge the accuracy and completeness of the information and have it amended as appropriate.

• **Correction — Article 4.9.5 Schedule 1 PIPEDA**

When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question.

• **Complain — Article 4.10 Schedule 1 PIPEDA**

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

• **Consent Withdrawal — Article 4.3.8 Schedule 1 PIPEDA**

An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.

2.4 Privacy Policy

Article 4.8 Schedule 1 PIPEDA requires an organization to be open about its policies and practices with respect to the management of personal information. The information made available shall include the name or title and the address of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded, the means of gaining access to personal information held by the organization, a description of the type of personal information held by the organization, and what personal information is made available to related organizations.

2.5 Direct Marketing

Article 6 of Canada's Anti-Spam Legislation (CASL) prohibits the sending, causing, or permitting of unsolicited electronic messages (including text, sound, voice, or image message) without express or implied consent. Messages must also identify the sender, contact information of the sender and an unsubscribe mechanism.

A telemarketer shall not initiate, and a client of a telemarketer shall make all reasonable efforts to ensure that the telemarketer does not initiate, a telemarketing telecommunication

to a consumer's telecommunications number that is on the National DNCL, unless express consent has been provided by such consumer to be contacted via a telemarketing telecommunication by that telemarketer or the client of that telemarketer.

Although postal marketing communications methods are not specifically regulated, it shall comply with the general requirements of Canadian Privacy Statutes.

2.6 Data Sharing and Processing

Under Canadian Privacy Statutes, an organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

Under PIPEDA, the Privacy Commissioner of Canada has the express authority to make arrangements concerning provincial data sharing and disclosure of information to foreign states for certain purposes.

2.7 Children's Privacy Protection

OPC's position is that organizations should avoid knowingly tracking children and tracking on websites aimed at children. OPC suggests that consent for the collection, use and disclosure of personal information of children under the age of 13 must be obtained from parents or guardians unless under exceptional cases. Young people above 13 but under the applicable age of majority can give meaningful consent, provided that their level of maturity is taken into consideration.

2.8 Accountability

a) Data Protection by Design & Default

There are no express provisions requiring privacy by design and default. However, OPC has released Reports of Findings addressing issues including default privacy settings, and the general principles of Canada Privacy Statutes, for instance openness, corresponds to the GDPR privacy by design & default principles.

b) Data Protection Impact Assessment (DPIA)

DPIAs are not mandatory for private sector organizations. Government institutions are required by the Treasury Board of Canada Secretariat to assess the privacy impacts of new or substantially modified programs or activities involving the creation, collection, and handling of personal information.

c) Record of Processing Activities

Not required.

d) Data Protection Officer (DPO)

Organizations are required to appoint an individual who is accountable for ensuring compliance with their data protection obligations. Such individuals are usually referred to as the Chief Privacy Officer or Privacy Officer.

e) Policies and Procedures

Organizations are required to implement policies and procedures to protect personal information, receive and respond to complaints and inquiries and to train staff.

2.9 Security and Data Breach Notification

Under the Canadian Privacy Statutes, the security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held. The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection.

For Alberta, an organization shall report to the OPC any breach of security safeguards involving personal information under its control if it is reasonable to believe that the breach creates a real risk of significant harm to an individual. Unless otherwise prohibited by law, the organization shall notify the individual affected. The notification shall contain certain prescribed information.

Under PIPEDA, notification of a privacy breach must be given to individuals, the OPC, and potentially other organizations (e.g. another organization, a government institution or a part of a government institution) if that organization, government institution or part concerned may be able to reduce the risk of the harm that could result from it or mitigate that harm, in the event of a breach of security safeguards if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual. Notification must be given as soon as feasible.

At the province level, notifications for data breaches relating to health information will also require notification to individuals or reporting to the relevant commissioners for that specific Industry.

2.10 Cross-border Data Transfer

In general, data transfer of personal information to a third-party processor outside Canada is permitted, provided that the transferring organization uses contractual or other means to provide a comparable level of protection while the information is being processed by a third party in a foreign jurisdiction.

In Alberta, more specifically, if an organization uses a service provider outside Canada to collect, use, disclose or store personal information, the organization must specify in its privacy policies and practices, the foreign jurisdictions in which the collection, use, disclosure or storage is taking place, and the purposes for which the foreign service provider has been authorized to collect, use or disclose personal information on its behalf.

2.11 Enforcement

OPC does not have the power to issue binding orders or fines as it is currently an ombudsperson. However, the provincial commissioners do have the abovementioned power. If a person contravenes PIPEDA's breach notification provisions may be regarded guilty of an offence punishable on summary conviction and liable to a fine not exceeding $10,000; or an indictable offence and liable to a fine not exceeding $100,000.

III. Asia-Pacific

1. Japan

1.1 Overview

1.1.1 Legal System

The Act on the Protection of Personal Information ("the APPI") is the main privacy legislation in Japan. The APPI was enacted in 2003 and amended respectively in December 2015 and June 2020[10]. There are also a number of Guidelines issued by the Personal Information Protection Committee ("the PPC") in relation to the implementation of the APPI. There are also other acts and guidelines for specific areas (such as financial, medical, employment, etc.) published jointly by the PPC and other ministries or independently by other ministries.

1.1.2 Supervisory Authorities

The PPC supervises the APPI's implementations and enforcements.

1.1.3 Material and Territorial Scope

The APPI applies to all business operators that handle personal information in Japan; for example, providing a personal information data base etc. for use in business. The definition of personal information handling business operator excludes central government, local government, and other administrative organs.

The APPI has extra-territorial application. According to Article 75 of the APPI, most of the articles regarding personal information handling business operators could apply to entities processing personal information outside of Japan but supplying a good or service to a person in Japan.

In addition, obligations regarding business operators who handle personal information specified in the chapter 4 of the APPI are not applicable to certain categories of such business operators, if the personal information is processed for the purpose set forth in Article 76 of APPI, for example, broadcasting institution, newspaper publisher or other press organizations process personal information for purpose of being provided for use in the press.

1.1.4 Data Processing Principles

Requirements set out in the Article 15 (Specifying a Utilization Purpose), Article 16 (Restriction due to a Utilization Purpose) and the Article 18 (Notification etc. of a Utilization

10 Please note that this Overview is only based on the 2020 amendments that will be effective since December 2020, while those may come into force in the spring of 2022 are not included.

Purpose when acquiring) of APPI reflects the principle regarding the limitations of personal information processing purpose (i.e. for specific purposes only).

1.1.5 Lawful basis for processing

According to the Article 17 (Proper Acquisition) of APPI, a business operator that handles personal information shall not acquire personal information by deceit or other improper means.

A business operator that handles personal information shall not acquire special care-required personal information without obtaining principal's (hereinafter, "principal" refers to the specific individual that can be identified through personal information) prior consent, except in situations set forth in the following:

(i) based on laws and regulations;

(ii) when it is necessary to protect a human life, body or fortune but is difficult to obtain principal's consent;

(iii) when there is a special need to enhance public health, or promote children's health but is difficult to obtain principal's consent;

(iv) when there is a need to cooperate with state government offices, local public entities or its trustees in their executions of affairs required by laws and regulations; however, obtaining the principal's consent may interfere with the execution of aforementioned affairs;

(v) when the special care-required personal information is publicly disclosed by the principal, state government offices, local public entities, entities specified in the Article 76 (1) of the APPI and other entities specified in Personal Information Protection Guidelines;

(vi) other situations prescribed by cabinet orders as similar to those situations set forth in preceding items.

1.2 Key Definitions

Personal information means information relating to a living individual and could identify a specific individual (including information which can be easily combined with other information to thereby identify a specific individual) or information containing an individual identification code.

Individual identification code means any character, letter, number, symbol or other codes a) into which a bodily partial feature of the specific individual has been converted in order

to be provided for use by computer and which could identify such specific individual, or b) which are assigned to when services or goods are provided to an individual or is recorded on a card or other documents issued to an individual to identify the person as a specific user.

Special care-required personal information refers to personal information comprising a principal's race, religion, social status, medical history, criminal record, fact of having suffered damage by committing a crime, or personal information prescribed by cabinet order as those of which the handling requires special care in order not to cause unfair discrimination, prejudice of other disadvantageous effects to the principal.

Controller and Processor: Instead of defining data controllers or processors directly, the APPI imposes requirements to business operators that handle personal information. Please see the above Section 1.1.3. Material and Territorial Scope for more details regarding the definition of business operators that handle personal information.

1.3 Data Subject Rights

According to Article 27 and Article 28 of the APPI, a principal could request to get informed about the utilization purposes of the personal information, and could demand business operators who handle personal information to disclose the personal information that can identify the principal among all the personal information obtained. Under Article 29 of the APPI, a principal can request business operator who handles personal information to correct, add or delete the personal information if it is incorrect. In accordance with Article 30(1) of the APPI, if the personal information is processed in violation of the Article 16 or 17 of APPI, the principal could request the business operators who handle personal information to cease its utilization of information or delete the personal information. Meanwhile, Article 30(3) provides that if the business operators who retain the personal information violate the Article 23(1) or 24 and provide the information to third parties, the identifying principal may request the business operators to stop such provisions.

According to Article 31 of the APPI, where the abovementioned rights are refused by the business operator that handles personal information, the business operator should strive to explain reasons to the principal.

According to the Article 61 of the APPI, the PPC may deal with necessary mediation affairs related to complaints lodged by a principal.

1.4 Privacy Policy

According to Article 27 of the APPI, privacy policies should include the following:

(i) the name or appellation and address and, for a corporate body, the name of its

representative of the said personal information handling business operator;

(ii) the utilization purpose of all personal data;

(iii) procedures for requesting access to personal information held by the business operator that handles personal information (including the amount of any fees payable);

(iv) besides those set forth under the preceding three items, those prescribed by cabinet order as a necessary matter to ensure the proper handling of retained personal information.

1.5 Direct Marketing

Direct marketing is subject to other laws (such as the Act on the Regulation of Transmission of Specified Electronic Mail and the Act on Specified Commercial Transaction).

1.6 Data Sharing and Processing

According to Article 23(1) of the APPI, a business operator who handles personal information shall not provide personal data to a third party without obtaining in advance a principal's consent, except in the following situations:

(i) based on laws and regulations;

(ii) when it is necessary to protect a human life, body or fortune but is difficult to obtain principal's consent;

(iii) when there is a special need to enhance public health, or promote children's health but it is difficult to obtain principal's consent;

(iv) when there is a need to cooperate with state government offices, local public entities, or its trustees in their executions of affairs required by laws and regulations; however, obtaining the principal's consent may interfere with the execution of aforementioned affairs.

There is no concept of "processor" under the APPI. Despite of that, according to Article 23(5), if (a) a personal information handling business operator entrusts all or part of the handling of personal data it acquires to an entity, (b) where personal data is provided accompanied with business succession caused by a merger or other reason, or (c) where personal data to be jointly utilized by a specified person is provided to the specified person, and when a principal has in advance been informed or a state has been in place where a principal can easily know to that effect as well as of the categories of the jointly utilized personal data, the scope of a jointly utilizing person, the utilization purpose for the utilizing person and the name or appellation of a person responsible for controlling the said personal data, the entity would

not be considered as a "third party" under Article 23(1) and Article 23(1) would not apply.

1.7 Children's Privacy Protection

There are no special rules regarding processing children's personal information. Nonetheless, please note that article 17 of APPI still applies to the processing of children's personal information and non-compliance actions could be deemed as "improper means of acquisition." Thus, it is practically recommended to obtain consents from the statutory guardians first.

1.8 Accountability

a) Data Protection by Design & Default

The APPI does NOT mention this concept.

b) Data Protection Impact Assessment (DPIA)

DPIAs are not explicitly required by APPI, but business operators that handle personal information should take necessary and appropriate actions for ensuring security, according to Article 20 of the APPI.

c) Record of Processing Activities

The APPI does not explicitly mention the obligation to record processing activities. However, according to Article 40, the PPC may inspect a book, document, and other property. In addition, Article 25 and Article 26 requires business operator that handles personal information to keep record when providing and receiving personal data to a third party.

d) Data Protection Officer (DPO)

Not required, but is recommended by the PPC according to its guidelines as a security measure.

1.9 Security and Data Breach Notification

Pursuant to the Measures in Correspondence to the Personal Data Breach[11], in case where a data breach occurs and there is a possibility of harming an individual's rights and interests as prescribed by rules of the PPC, the business operator that handles personal information shall report to the PPC of such, and shall notify the principal of the occurrence of the said situation.

11 uahttps://www.ppc.go.jp/files/pdf/iinkaikokuzi01.pdf

1.10 Cross-border Data Transfer

According to Article 24 of the APPI, if a business operator that handles personal information provides personal information to an oversea third party, it shall in advance obtain a principal's consent, unless:

a) the third party establishes a necessary system conforming to standards prescribed by rules of the APPI as necessary for continuously taking equivalent measures to the APPI; or

b) the foreign country is prescribed by rules of the PPC as a foreign country with a personal information protection system recognized to have equivalent standards as Japan.

1.11 Enforcement

The highest penalty of violating APPI could reach 100 million yen fine, or a limited term of imprisonment for up to two years.

2. Hong Kong

2.1 PDPO Overview

2.1.1. Legal System

The Personal Data (Privacy) Ordinance (Cap. 486) ("PDPO") regulates the use of personal data by data users. The PDPO sets out six data protection principles ("DPPs") (see Section 2.1.4 below) as well as other data protection requirements on data users (e.g. direct marketing, see Section 2.5 below).

The Privacy Commissioner for Personal Data enforces the provisions of the PDPO. The Privacy Commissioner also endorses voluntary Codes of Practice where compliance is not legally required under the PDPO but non-compliance with the same may lead to investigatory actions by the Privacy Commissioner and a presumption against the relevant data user in court proceedings.

2.1.2 Supervisory Authorities

Privacy Commissioner for Personal Data ("PCPD"), Hong Kong

2.1.3 Material and Territorial Scope

Material Scope - The PDPO applies to the collection, retention, processing and use of personal data in Hong Kong. "Processing" is defined to include amending, augmenting, deleting, or rearranging the data, whether by automated means or otherwise, while "use" is defined to include disclosure or transfer of personal data. See item ii.1 below for definition of "Personal Data".

Territorial Scope - The PDPO applies to the collection, holding, processing or use of personal data that takes place in Hong Kong or is controlled by a data user in Hong Kong (see item ii.2 below for definition of "data user"). The PDPO does not have extra-territorial application.

2.1.4 Data Protection Principles

DPP1: Purpose and manner of collection of personal data

Personal data collected must be necessary for a lawful purpose directly related to a function or activity of the data user. It must also be adequate but not excessive in relation to that purpose. Data user must inform the data subject of certain prescribed information (see item iv below).

DPP2: Accuracy and duration of retention of personal data

Data users should ensure that personal data is accurate and should not be kept for longer than is necessary. Data processors engaged must be contractually required to comply with this DPP.

DPP3: Use of personal data

Data users must not use personal data for a new purpose unless the express consent from the data subject is obtained.

DPP4: Security of personal data

Practical steps must be taken to safeguard personal data from unauthorized or accidental access, processing, erasure having particular regard to a number of prescribed factors. Data processors engaged must be contractually required to comply with this DPP.

DPP5: Information to be generally available

A data user must make certain information available, such as its policies and practices in relation to personal data.

DPP6: Access to personal data

Data subjects must be given data access and correction rights in relation to their personal data.

2.1.5 Lawful basis for processing

The PDPO does not prescribe the specific "lawful basis" for processing of personal data. Under the PDPO, consent from data subjects is generally not required for the use of personal data, provided that the data user complies with the statutory requirement to notify data subjects of certain prescribed information (see item iv below). Consent is generally only required where personal data is used for: (i) direct marketing; (ii) new purpose; and (iii) matching procedure. That said, where consent is required, certain exemptions are available under the PDPO (e.g. for purposes of prevention of crime, statistics and research, news, health etc.).

2.2 Key Definitions

a) Personal Data and Special Categories of Personal Data

Personal data is defined as any data which (a) relates directly or indirectly to a living

individual; (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and (c) in a form in which access to or processing of the data is practicable. There is no separate category for sensitive personal data under the PDPO.

b) User and Processor

Data user means a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data.

Data processor means a person who (a) processes personal data on behalf of another person; and (b) does not process the data for any of the person's own purposes.

2.3 Data Subject Rights

The PDPO specifically prescribes two (2) rights for data subjects:

(a) Data Access Request ("DAR") rights

Data subjects have the right to request access to the personal data held by the data user of which he is the data subject.

(b) Data Correction Request ("DCR") rights

Data subjects have the right to request correction of the personal data held by the data user of which he is the data subject.

Within 40 days from receiving the DAR or DCR, the data user must either comply with the same or, if it is unable to comply, respond to the individual stating the reason(s) (e.g. more time is required).

2.4 Privacy Policy

DPP1 and DPP5 of the PDPO require data users to notify data subjects of certain prescribed information such as the types of personal data collected, the purposes of collection, whether it is obligatory for data subject to supply such data (and if so, the consequences of not supplying), the classes of transferee to whom such data may be transferred to, the data subjects' data access and correction rights and details of the relevant contact person. Such information is commonly included in a data user's privacy policy made available to data subjects.

2.5 Direct Marketing

Marketing constitutes direct marketing ("DM") if the method of marketing falls under any of the following:

(a) sending information or goods, addressed to specific persons by name, by mail, fax, electronic mail, or other means of communication; or

(b) making telephone calls to specific persons.

Express consent from the data subjects is required before a data user can (i) use personal data for DM purposes; or (ii) supply personal data to others for their DM purposes. Data users must also notify data subjects of certain prescribed information (e.g. kinds of personal data that will be used for DM, the types of goods or services that will be marketed to the individual etc.)

2.6 Data Sharing and Processing

DPP1 requires data users to inform data subjects of the classes of transferee to whom the personal data may be transferred to. Such classes of transferees should be clearly defined so that they can be ascertained with a reasonable degree of certainty.

In relation to all data sharing and processing where data processors are engaged, DPP2 and DPP4 require data users to contractually bind such data processors to comply with data retention and security requirements under the PDPO. There is currently no fixed template or modal clauses for such agreement with data processors under PDPO.

2.7 Children's Privacy Protection

The collection of minor's personal data remains subject to the general requirements under the PDPO. Note, in particular, that collection of personal data must be fair, necessary, and not excessive in the circumstances of the case involving minors.

Where consent is required under the PDPO (e.g. use of personal data for a new purpose), a relevant person (i.e. a person who has parental responsibility for the minor) will be able to provide such consent on behalf of the minor. However, the data user must not use such personal data for a new purpose (even with the consent of the relevant person) unless he has reasonable grounds for believing that the use of that data for the new purpose is clearly in the interest of the minor.

The PDPO also prescribes an exemption from consent requirement for disclosure of minor's personal data by the Hong Kong Police Force or Customs and Excise Department to a relevant person of the minor.

2.8 Accountability

a) Data Protection by Design & Default

There is no legal requirement under the PDPO for data protection by design and default. However, it is a good practice recommended by the PCPD in particular in relation to the roll out of new information and communication technologies.

b) Data Protection Impact Assessment (DPIA)

There is no legal requirement under the PDPO for DPIA to be conducted. However, the PCPD has issued an information leaflet on Privacy Impact Assessments and recommends conducting PIAs in certain circumstances e.g. processing of large amounts of personal data or the implementation of privacy intrusive technologies.

c) Record of Processing Activities

Not applicable for Hong Kong.

d) Data Protection Officer (DPO)

Not applicable for Hong Kong.

2.9 Security and Data Breach Notification

The PDPO currently does not prescribe security and data breach notification requirements, although the Privacy Commissioner has set up a voluntary online data breach notification platform where data users are advised to do so as a recommended practice for proper handling of such incident. The Privacy Commissioner has also issued a non-binding Guidance on Data Breach Handling and the Giving of Breach Notifications.

2.10 Cross-border Data Transfer

The express provision under the PDPO (i.e. section 33 PDPO) dealing with overseas transfer of personal data has yet to be in force. Nonetheless, as "use" is defined to include transfer under the PDPO, such transfer remains subject to the general regulation of personal data under the PDPO.

2.11 Enforcement

The Privacy Commissioner typically adopts a conciliation approach for any disputes involving personal data between parties. For serious cases, the Privacy Commissioner will conduct

investigations followed by the issuance of warnings or legal enforcement notices under the PDPO. Breach of the DPPs per se do not constitute criminal offences, but breach of an enforcement notice issued by the Privacy Commissioner is an offence carrying a maximum fine of HK$50,000 (approx. US$6,400) and imprisonment of 2 years (on first conviction). In addition, breach of direct marketing provisions under the PDPO also constitutes an offence which carries a maximum fine of HK$1 million (approx. US$128,000) and imprisonment of 5 years. In relation to breach of the offences for disclosing personal data obtained without consent from data users, the offence carries a maximum fine of HK$1 million (approx. US$128,000) and imprisonment of 5 years.

环球律师事务所 GLOBAL LAW OFFICE SINCE 1979
环球律师事务所 GLOBAL LAW OFFICE SINCE 1979

3. Singapore

3.1 Overview

3.1.1 Legal System

The main data protection legislation in Singapore is the Personal Data Protection Act 2012 ("PDPA"). In addition to the PDPA, the data protection regime in Singapore also consists of various general and sector-specific guidelines issued by the Personal Data Protection Commission ("PDPC"). While these guidelines are not legally binding, they indicate the manner in which the PDPC will interpret the PDPA and set out best practices applicable to personal data processing in Singapore.

3.1.2 Supervisory Authorities

The PDPC is responsible for enforcing the PDPA.

3.1.3 Material and Territorial Scope

a) Material Scope

The PDPA applies generally to the processing of personal data (see definition of "personal data" in section ii.1 below), but not in relation to the following situations:

- any individual acting in a personal or domestic capacity;
- any employee acting in the course of his or her employment with an organization (although the organization will remain responsible for compliance with the PDPA);
- any public agency or organization in the course of acting on behalf of a public agency in relation to the collection, use or disclosure of personal data; and
- the processing of business contact information, which refers to an individual's name, position name or title, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his or her personal purposes.

In addition, there are several exceptions to the PDPA's data protection obligations set out in the Second to Sixth Schedules of the PDPA. For example, organizations are allowed to collect personal data without consent if this is necessary for any investigations or proceedings or if the personal data is publicly available.

b) Territorial Scope

The PDPA applies to any organization, including an entity based outside of Singapore, which carries out the collection, use or disclosure of personal data in Singapore. However, in practice, organizations would require a Singapore link (e.g. incorporation in Singapore or having a presence in Singapore) in order for the PDPA to be enforceable against them.

3.1.4 Data Processing Principles

The PDPA sets out 9 data processing principles which organizations will need to comply with when processing personal data:

- Consent obligation: an organization must obtain the consent of the individual before collecting, using, or disclosing personal data;
- Purpose limitation obligation: an organization may collect, use, or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances and, where applicable, such purposes have been notified to the individual concerned;
- Notification obligation: an organization must notify the individual of the purpose(s) for which it intends to collect, use, or disclose personal data, on or before such collection, use or disclosure of personal data;
- Access and correction obligations: upon request by the relevant individual, an organization must provide information in which the individual's personal data have been used or disclosed by the organization and correct any error or omission in the individual's personal data;
- Accuracy obligation: an organization must make a reasonable effort to ensure that the personal data collected by the organization is accurate and complete;
- Protection obligation: an organization must protect personal data in its possession or control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal, or other similar risks;
- Retention limitation obligation: an organization must cease to retain personal data or remove the means by which he personal data can be associated with particular individuals if the purpose for which the personal data was collected is no longer being served by the retention of personal data, or if the retention is no longer necessary for legal or business purposes;
- Transfer limitation obligation: an organization must ensure that any personal data transferred outside Singapore is conferred a standard of protection that is comparable to

the standard of protection under the PDPA; and

- Accountability obligation: an organization must implement the necessary policies and procedures to meet its obligations under the PDPA, and make information about its policies and practices publicly available.

An organization which is deemed to be a data intermediary (see definition of "data intermediary" in section ii.2 below) and processes personal data on behalf of and for the purposes of another organization pursuant to a written contract is subject only to the protection and retention limitation obligations under the PDPA.

3.1.5 Lawful Basis for Processing

An organization may only collect, use, or disclose personal data in any one of the following scenarios:

- express consent is obtained from the individual, provided that: (i) the purposes for the collection, use or disclosure of personal data has been notified to the individual and (ii) the individual cannot be required to consent to the collection, use or disclosure of personal data for purposes which go beyond what is reasonable to provide a product or service to the individual;

- there is deemed consent by the individual to the collection, use or disclosure of personal data – this arises where the individual voluntarily provides personal data to the organization for a particular purpose, and it is reasonable from the circumstances that the individual would voluntarily provide the data for this purpose; or

an exception to the consent obligation (as set out in the Second to Fourth Schedules of the PDPA) applies.

3.2 Key Definitions

3.2.1 Personal Data and Special Categories of Personal Data

Personal data is defined as "data, whether true or not, about an individual who can be identified (a) from that data or (b) from that data and other information to which an organization has or is likely to have access".

There is no definition of sensitive personal data or specific rules for special categories of personal data in the PDPA. However, guidance from the PDPC does suggest that personal data of a sensitive nature should be accorded a higher level of protection as a matter of good practice.

3.2.2 Controller and Processor

A concept similar to that of a controller under the PDPA is an "organization", which includes "any organization, company, association or body of persons, corporate or unincorporated, whether or not (a) formed or recognized under the law of Singapore; or (b) resident, or having a place of business, in Singapore".

A concept similar to that of a processor under the PDPA is a "data intermediary", which means "an organization which processes personal data on behalf of another organization but does not include an employee of that other organization".

3.3 Data Subject Rights

Individuals have the following rights under the PDPA:

- Right to access their personal data;
- Right to correct their personal data; and
- Right to withdraw their consent to the collection, use or disclosure of their personal data.

An organization must comply with any access or correction requests "as soon as reasonably possible from the time the access request is received" and generally within 30 days, although there is a possibility to extend this. An organization is not obligated to respond to an access or correction request if an exception to the access or correction obligation (as set out in the Fifth and Sixth Schedules of the PDPA) applies. An organization may charge a reasonable fee to process an access or correction request by the individual.

An organization must comply with any notice from an individual to withdraw his or her consent to the collection, use or disclosure of personal data generally within 10 business days from the day the organization receives the withdrawal notice, although there is a possibility to extend this.

The PDPA is presently being amended to introduce a new right to data portability, i.e. an organization must, at the individual's request, provide the individual's data that is in the organization's possession or control, in a commonly used machine-readable format.

3.4 Privacy Notice

The PDPA requires organizations to: (a) notify individuals of the purposes for the collection, use or disclosure of personal data; and (b) on request by the individual, provide the business contact information of a person who is able to answer on behalf of the organization questions

about the collection, use or disclosure of personal data.

In practice, both of (a) and (b) will be set out in a privacy notice (or privacy policy) given to individuals on or before the collection, use or disclosure of personal data.

3.5 Direct Marketing

Telephone marketing (including text messages and faxes) is governed by the Do-Not-Call ("DNC") provisions of the PDPA. A person can only send marketing messages to a Singapore telephone number that is listed on the DNC register if there is, amongst other things, clear and unambiguous consent from the relevant subscriber or user or if there is an ongoing business relationship.

Email marketing is governed by the Spam Control Act. Unsolicited email marketing messages may be sent in bulk to individuals if the email complies with the requirements set out in the Spam Control Act, including a labelling requirement and a requirement to provide an unsubscribe facility. An organization must cease to send marketing emails to a particular individual 10 business days after it receives an unsubscribe request from that individual.

It should be noted that the PDPC has announced plans to merge the DNC provisions under the PDPA with the Spam Control Act.

3.6 Data Sharing and Processing

An organization remains responsible for any personal data processed on its behalf by a data intermediary as if the personal data were processed by the organization itself. To this end, most organizations will enter into data processing agreements with their data intermediaries and seek to flow through their primary PDPA obligations to ensure that the processing of personal data by the data intermediary complies with the PDPA.

3.7 Children's Privacy Protection

Guidelines published by the PDPC set out additional non-binding requirements applicable to the processing of personal data in relation to children. The PDPC generally considers a minor who is at least 13 years old to be able to consent on his or her behalf. However, organizations should nevertheless ensure that minors have a sufficient understanding of the nature and consequences of giving consent when determining whether consent is valid.

The PDPC guidelines also advise organizations to have in place precautions when collecting, using, or disclosing personal data (including ensuring that the language is clear and understandable) and take extra steps to verify the accuracy of personal data, particularly where an inaccuracy could have severe consequences for the minor.

3.8 Accountability

a) Data Protection by Design & Default

There is no express data protection by design & default provision in the PDPA, but the PDPC considers it good practice for an organization to have appropriate policies and processes in place before it embarks on any data processing. To this end, the PDPC has released a Guide to Data Protection by Design for ICT Systems, which incorporates data protection by default as one of the overarching principles.

b) Data Protection Impact Assessment (DPIA)

There is no mandatory requirement to conduct DPIAs in the PDPA. However, the PDPC encourages organizations to conduct DPIAs when systems or processes are new and in the process of being designed or in the process of undergoing major changes as doing otherwise may lead to increased costs and effort. The person leading this effort should ideally be the Data Protection Officer ("DPO") or the project manager.

c) Record of Processing Activities

There is no legal requirement to maintain a record of processing activities.

d) Data Protection Officer ("DPO") and GDPR Representative

There is a legal obligation for an organization to appoint a DPO. The business contact information of the DPO must be made available to the public.

There is no equivalent concept of a "representative" (i.e. a requirement for organizations based outside of Singapore to appoint a Singapore-based point of contact to handle data protection matters) in the PDPA.

3.9 Security and Data Breach Notification

Although there is currently no mandatory data breach notification requirement under the PDPA, the PDPC recommends organizations to notify the PDPC (as soon as practicable, and generally no later than 72 hours from the time the organization has assessed the breach to be notifiable) where the data breach is:

- of a significant scale (i.e. the data breach involves the personal data of 500 or more individuals); or

- likely to result in significant harm or impact to the individuals to whom the data relates.

In this case, the PDPC also recommends organizations to notify the affected individuals (as soon as practicable).

(collectively, "Voluntary Breach Notification Requirements").

Although the Voluntary Breach Notification Requirements are not legally binding, in practice, most organizations would seek to comply with them as though they were a mandatory requirement once the breach is assessed to have met the notification thresholds. This is because organizations are concerned with the reputational fallout and negative reaction from customers if they are perceived to be not in compliance with the Voluntary Breach Notification Requirements. In addition, the PDPC has indicated that the lack of notification would be taken into account by the PDPC in determining whether to take any regulatory action against an organization as a result of the breach.

Please note that the PDPA is presently being amended to introduce a mandatory data breach notification regime. The notification thresholds / timelines under the proposed regime are expected to be similar to the current Voluntary Breach Notification Requirements.

3.10 Cross-border Data Transfer

Cross-border data transfers are permitted under the PDPA, but the organization will need to ensure that the recipient of the data confers on the personal data a standard of protection that is comparable to that under the PDPA. This can be achieved by, among other things:

- entering into a data processing agreement requiring the recipient to provide the personal data with a level of protection that is comparable to the PDPA;
- verifying that the applicable law in the jurisdiction that the personal data will be transferred to provides a level of protection that is comparable to the PDPA; or

obtaining the individual's consent to the transfer, subject to such consent satisfying certain prescribed conditions.

3.11 Enforcement

Non-compliance with the data protection obligations may result in:

- fines of up to SGD 1 million;
- directions from the PDPC to stop collecting, using, or disclosing the personal data;
- directions from the PDPC to destroy the personal data; and/or

• directions from the PDPC to provide or refuse access or correction of the personal data.

The PDPA is presently being amended to increase the maximum fine to up to 10% of an organization's annual gross turnover in Singapore or SGD 1 million, whichever is higher.

In addition, individuals have the rights to lodge a complaint with competent the PDPC, to seek effective judicial remedy, and to obtain an injunction or receive damages from an organization for any loss suffered as a result of the organization's infringement of the PDPA.

环球律师事务所 GLOBAL LAW OFFICE SINCE 1979
环球律师事务所 GLOBAL LAW OFFICE SINCE 1979

4. Malaysia

4.1 Overview

4.1.1 Legal System

The main legislation governing data protection in Malaysia is the Personal Data Protection Act 2010 ("PDPA"), which is supported by the Data Protection Regulations 2013 ("PDP Regulations").

4.1.2 Supervisory Authorities

The data protection regulatory body of Malaysia is the Jabatan Perlindungan Data Peribadi ("JPJD"), which is an agency under the Ministry of Communications and Multimedia Commission.

4.1.3 Material and Territorial Scope

a) Material Scope

The PDPA applies in respect to the processing of personal data (see definition of "personal data" in section ii.1 below), but not to the processing of personal data by the Federal and State governments. It should be noted that the JPJD has proposed to amend the PDPA to exempt business contact information from the application of the PDPA.

b) Territorial Scope

The PDPA applies to data users if they are:

- established in Malaysia and the personal data is processed, whether or not in the context of that establishment, by that person or any other person employed or engaged by that establishment; or
- not established in Malaysia, but use equipment in Malaysia for processing the personal data otherwise than for purposes of transit through Malaysia.

4.1.4 Data Processing Principles

The PDPA sets out 7 data processing principles which organizations will need to comply with when processing personal data:

- General Principle: personal data can only be processed with the consent of the data subject or if an exception to the consent requirement applies;

Notice and Choice Principle: a data user must serve a written notice to the data subject;

- Disclosure Principle: personal data cannot be disclosed to third parties without the knowledge and consent of the data subject;

- Security Principle: a data user must take practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration, or destruction;

- Retention Principle: personal data processed for any purpose must not be kept longer than is necessary for the fulfilment of that purpose;

- Data Integrity Principle: a data user must take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept up-to-date; and

- Access Principle: a data subject must be given access to his or her personal data held by a data user and be able to correct that personal data where it is inaccurate, incomplete, misleading, or not up-to-date.

4.1.5 Lawful Basis for Processing

Personal data must not be processed unless consent is given by the data subject, the data is processed for a lawful purpose directly related to an activity of the data user, the processing is necessary for the purpose, and the data processed is adequate but not excessive. However, personal data may be processed without consent in certain circumstances, including:

- where it is necessary for the performance of or entering into a contract that a data subject is a party;

- for compliance with legal obligations;

- for the administration of justice;

- to protect the vital interests of the data subject; and

- for the exercise of any functions conferred on any person by or under any written law.

Sensitive personal data may only be processed with the data subject's explicit consent or where it is necessary for:

- performing rights or obligations in connection with employment;

- protecting the vital interests of another person where consent reasonably be obtained (or given by the data subject);
- medical purposes undertaken by a healthcare professional or someone with a duty of confidentiality;
- obtaining legal advice, exercising legal rights, and situations in connection with legal proceedings;
- the administration of justice;
- the exercise of any functions conferred on any person by or under any written law; and any other purposes as the Minister thinks fit.

4.2 Key Definitions

4.2.1 Personal Data and Special Categories of Personal Data

Personal data is defined as "any information in respect of commercial transactions, which (a) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose; (b) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system", and in each case that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user. Personal data includes any sensitive personal data and expression of opinion about the data subject, but does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010.

Sensitive personal data means "any personal data consisting of information as to the physical or mental health or condition of a data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offence or any other personal data as the Minister may determine by order published in the Gazette."

4.2.2 Controller and Processor

A concept similar to that of a controller under the PDPA is a "data user", which is "a person who either alone or jointly or in common with other person's processes and personal data or has control or authorizes the processing of any personal data, but who does not include a processor".

A data processor is defined as "any person, other than an employee of the data user, who processes the personal data solely on behalf of the data user, and does not process the personal data for any of his own purposes".

4.3 Data Subject Rights

Individuals have the following rights under the PDPA:

- Right to access their personal data;
- Right to correct their personal data;
- Right to prevent the processing of personal data for the purposes of direct marketing; and

Right to withdraw their consent to the collection, use or disclosure of their personal data.

An organization must comply with any access or correction requests within 21 days from the date of receipt of the request, although there is a possibility to extend this. An organization is not obligated to respond to an access or correction request if an exception to the access or correction obligation applies (e.g. the data user is not supplied with information as it may reasonable require to locate the personal data to which the access request relates or to ascertain in what way to which the personal data to which the correct request relates is inaccurate, incomplete, misleading or out of date). An organization may charge a reasonable fee to process an access or correction request by the individual, with the maximum fee fixed by subsidiary regulations under the PDPA.

It should be noted that the JPJD has proposed to amend the PDPA to introduce a new right to data portability, i.e. individuals will have the right to access his or personal data in a structured, machine-readable format which can be transferred from one data user to another data user to obtain services.

4.4 Privacy Notice

Under the Notice and Choice principle, a data user must provide a data subject with:

- a description and source of the personal data to be processed by the data user;
- the purpose of processing, the data subject's rights;
- the class of third parties that the data may be disclosed to;
- the choices and means of limiting the processing of the data;

- whether it is obligatory or voluntary for the data user or data subject to supply the data; and

- the consequences for failing to supply the data.

The notice must be given as soon as practicable and in both the English language and Bahasa Malaysia.

4.5 Direct Marketing

A data subject has the right to prevent the processing of his or her personal data for direct marketing, whether to cease or not to begin processing personal data, by submitting a notice in writing to the data user. It should be noted that the JPJD is currently reviewing the legal regime applicable to direct marketing, and there have been proposals to (among other things) set up a Do-Not-Call registry and require data users to implement a mechanism for data subjects to unsubscribe from online services.

4.6 Data Sharing and Processing

Personal data cannot be disclosed to third parties without the knowledge and consent of the data subject. However, personal data may be disclosed without consent if:

- the disclosure (a) is necessary for the purpose of preventing or detecting a crime, or for the purpose of investigations; or (b) was required or authorized by or under any law or by the order of a court;

- the data user acted in the reasonable belief that he had in law the right to disclose the personal data to the other person;

- the data user acted in the reasonable belief that he would have had the consent of the data subject if the data subject had known of the disclosing of the personal data and the circumstances of such disclosure; or

- the disclosure was justified as being in the public interest in circumstances as determined by the Minister.

Where the processing is carried out by a data processor, the data user must ensure that the data processor provides sufficient guarantees in respect of technical and organizational security measures governing the processing, and take reasonable steps to ensure compliance with those measures.

4.7 Children's Privacy Protection

The PDP Regulations provide that for data subjects below the age of 18 years, consent must be given by the parent, guardian, or someone who has parental responsibility for the data subject. Apart from this, there are no other special rules applicable to the processing of the personal data of children.

4.8 Accountability

a) Data Protection by Design & Default

There is no express data protection by design & default provision in the PDPA, but a data user is required under the Security Principle to take practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration, or destruction. Where the processing is carried out by a data processor, the data user must ensure that the data processor provides sufficient guarantees in respect of technical and organizational security measures governing the processing, and take reasonable steps to ensure compliance with those measures.

It should be noted that the JPJD has announced plans to issue guidelines to guide the implementation of privacy by design by data users.

b) Data Protection Impact Assessment (DPIA)

There is no legal requirement to conduct DPIAs.

c) Record of Processing Activities

A data user is required to keep and maintain a record of any application, notice, request, or any other information relating to personal data that has been or is being processed by it.

d) Data Protection Officer ("DPO") and GDPR Representative

There is no presently legal obligation for data users to appoint a DPO, but the JPJD has announced plans to amend the PDPA to impose a mandatory obligation on data users to appoint a DPO.

A data user will need to nominate a representative established in Malaysia where the data user is not established in Malaysia but uses equipment in Malaysia for the processing of personal data (other than for the purposes of transit through Malaysia).

4.9 Security and Data Breach Notification

There is currently no mandatory data breach notification requirement, although the JPJD

has announced plans to amend the PDPA to introduce a mandatory data breach notification requirement.

4.10 Cross-border Data Transfer

A data user can transfer personal data to a location outside Malaysia if:

- the location is whitelisted by the Minister and published in the Gazette (however it should be noted that no such location have been gazetted yet);
- the data subject has given his consent to the transfer;
- the transfer is necessary for the performance of a contract between the data subject and the data user;
- the transfer is necessary for the conclusion or performance of a contract between the data user and a third party which (i) is entered into at the request of the data subject; or (ii) is in the interests of the data subject;
- the transfer is for the purpose of any legal proceedings or for the purpose of obtaining legal advice or for establishing, exercising, or defending legal rights;
- the data user has reasonable grounds for believing that in all circumstances of the case (i) the transfer is for the avoidance or mitigation of adverse action against the data subject; (ii) it is not practicable to obtain the consent in writing of the data subject to that transfer; and (iii) if it was practicable to obtain such consent, the data subject would have given his consent;
- the data user has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not in that place be processed in any manner which, if that place is Malaysia, would be a contravention of the PDPA;
- the transfer is necessary in order to protect the vital interests of the data subject; or
- the transfer is necessary as being in the public interest in circumstances as determined by the Minister.

In practice, most data users in Malaysia will rely on the mechanism, where the data user will take all reasonable precautions and exercise all due diligence to ensure that the personal data will not be processed illegally, as a basis for transferring personal data outside Malaysia and enter into a data transfer agreement with recipients of the data to ensure that the personal data will not be processed in a manner that contravenes the PDPA.

4.11 Enforcement

Non-compliance with the data protection obligations may result in fines of up to RM 500,000 and/or imprisonment of up to 3 years. Persons responsible for the management of the affairs of a corporate body, at the time an offence was committed by the corporate body, may also be charged severally or jointly in the same proceedings.

It should be noted that the JPJD has announced plans to amend the PDPA to introduce a right for data subjects to take civil action against a data user for breaching the PDPA.

环球律师事务所 GLOBAL LAW OFFICE SINCE 1979

5. Thailand

5.1 Overview

5.1.1 Legal System

The main legislation governing data protection in Thailand is the Personal Data Protection Act B.E. 2562 (2019) ("PDPA"). It should be noted that the Thai Government has postponed the enforcement of the key obligations in the PDPA imposed on data controllers and processors to 27 May 2021.

5.1.2 Supervisory Authorities

The regulator responsible for enforcing the PDPA is the Personal Data Protection Commission ("PDPC").

5.1.3 Material and Territorial Scope

a) Material Scope

The PDPA applies in respect to the processing of personal data (see definition of "personal data" in Section 5.2.1 below), but not in relation to the following situations:

the collection, use or disclosure of personal data by a person who collects such personal data for personal benefit or household activities;

- the operations of public authorities who are under a duty to maintain state security, including the financial security of the state or public safety, such as duties with respect to the prevention and suppression of money laundering, forensic science, or cybersecurity;

- a person or a juristic person who uses or discloses personal data that is collected only for the activities of mass media, fine arts, or literature, provided that these are in accordance with professional ethics or for the public interest;

- the collection, use or disclosure of personal data by the House of Representatives, the Senate, and the Parliament in accordance with their duties and powers;

- the trial and adjudication of courts and work operations of officers in legal proceedings, legal execution, and deposit of property, including work operations in accordance with the criminal justice procedure; and

- operations of data undertaken by a credit bureau company and its members in accordance with the law governing the operations of a credit bureau business.

b) Territorial Scope

The PDPA applies to the processing activities of a controller or processor who has an establishment in Thailand, and also to the processing activities of a controller or processor based outside Thailand to the extent that it:

- offers products or services to data subjects, irrespective of whether payment is made by the data subject; or
- monitors the behavior of data subjects in Thailand.

5.1.4 Data Processing Principles

The PDPA sets out 8 data processing principles which organizations will need to comply with when processing personal data:

- personal data must be processed under a lawful basis.
- personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- personal data must be adequate, relevant, and limited to what is necessary in relation to purposes for which they are processed.
- personal data must be accurate and kept up to date.
- personal data must be kept for no longer than is necessary.
- personal data must be processed in accordance with the individual's rights
- personal data must be kept secure.
- personal data must not be transferred to third countries which do not provide adequate protection.

5.1.5 Lawful basis for processing

Generally, personal data must not be processed unless consent is given by the data subject. However, personal data may be processed without consent in certain circumstances, including:

- to prepare a historical document or statistical study;

- to protect the vital interests of an individual;
- to undertake any necessary contractual obligation between the individual and the controller, or to comply with the individual's request prior to entering into such contract;
- to undertake any necessary obligation of the controller in relation to public interest;
- for a legitimate interest of any individual or juristic person (including the controller); or
- to undertake any legal obligation of the controller.
- Sensitive personal data can only proceed with the data subject's explicit consent or where the processing of such data is:
- to prevent or suppress danger to life, body, or health to a person where the data
- subject is incapable of giving consent;
- carried out in the course of legitimate activities with appropriate safeguards by non-profit bodies (such as those with a political, religious, or philosophical purpose);
- in relation to information that has been disclosed to the public with the explicit consent of the data subject;
- necessary for the purpose of legal claims; or
- for compliance with laws with purposes including, amongst others, public interest in public health, employment protection, and certain research purposes.

5.2 Key Definitions

5.2.1 Personal Data and Special Categories of Personal Data

Personal data is defined as "any information relating to a Person, which enables the identification of a Person, whether directly or indirectly, but does not include the information of deceased Persons."

The term "sensitive personal data" is not used in the PDPA, but the law does subject the processing of certain categories of sensitive data to a higher standard. This includes data pertaining to "racial, ethnic origin, political opinions, cult, religious or philosophical beliefs, sexual behavior, criminal records, health data, disability, trade union information, genetic data, biometric data, or of any data which may affect the data subject in the same manner."

The PDPC is expected to provide further guidance on this in subsidiary legislation issued under the PDPA.

5.2.2 Controller and Processor

A data controller means "a Person or a juristic person having the power and duties to make decisions regarding the collection, use, or disclosure of the Personal Data."

A data processor means "a Person or a juristic person who operates in relation to the collection, use, or disclosure of the Personal Data pursuant to the orders given by or on behalf of a Data Controller, whereby such Person or juristic person is not the Data Controller."

A "Person" and is defined in the PDPA as "a natural person".

5.3 Data Subject Rights

Individuals have the following rights under the PDPA:

- Right to access their personal data;
- Right to request the controller to rectify the personal data to ensure that it remains accurate, up-to-date, complete, and not misleading;
- Right to data portability, i.e. to receive their personal data in a format which is readable or commonly used by way of automatic tools and can be used or disclosed by automated means;
- Right to object to the collection, use or disclosure of personal data; and
- Right to restrict the use of his or her personal data.

Requests to exercise data subject rights could be limited in certain circumstances (e.g. right to access or data portability should not violate the rights or freedoms of others). The PDPC is expected to provide further guidance on data subject rights (including the timelines applicable to responding to data subject requests) in subsidiary legislation issued under the PDPA.

5.4 Privacy Notice

A data subject must be informed or aware of the information listed below on or before the collection of personal data:

- the purpose of the processing of his/her personal data;
- whether the collection of personal data is a legal or contractual requirement, or a requirement necessary to enter into a contract, as well as the possible consequences where the data subject fails to provide such data;
- the personal data to be collected and the retention period for such personal data
- the categories of person or entities to whom the personal data may be disclosed to;
- the identity and contact details of the data controller and where applicable, the controller's representative or data protection officer ("DPO"); and
- the rights of the data subject.

5.5 Direct Marketing

Under the PDPA, a data subject may object to the processing of his or her Personal Data for the purposes of direct marketing. There are no general rules for telephone marketing, but there are certain sector-specific regulations in industries such as insurance or finance. Direct email marketing is allowed provided the receiver can easily opt-out and unsubscribe from such emails.

5.6 Data Sharing and Processing

Where Personal Data is to be provided to other Persons and legal persons other than the Data Controller, the Data Controller must "take action" to prevent the Persons and legal persons from disclosing the data unlawfully. The PDPC is expected to provide further guidance on this in subsidiary legislation issued under the PDPA.

5.7 Children's Privacy Protection

If the data subject is between 10 and 20 years old, consent must be obtained from the data subject together with the data subject's legal guardian, unless it relates to an act that a minor is permitted to perform on his or her own under Sections 22 to 24 of Thailand's Civil and Commercial Code.

If the data subject is below 10 years old, consent must be obtained from the data subject's legal guardian.

5.8 Accountability

a) Data Protection by Design & Default

There is no express data protection by design & default provision in the PDPA.

b) Data Protection Impact Assessment (DPIA)

There is no legal requirement to conduct DPIAs, although data controllers are required to review security measures when necessary or when the "technology has changed". The PDPC is expected to provide further guidance on this in subsidiary legislation issued under the PDPA.

c) Record of Processing Activities

Unless the data controller is a "small organization" as prescribed by the PDPC, it is required to maintain a record of the following information:

- personal data collected;
- the purpose of collection of the data in each category;
- details of the Data Controller;
- retention period for the personal data;
- rights and methods of access to the personal data, including the conditions used to assess whether a person has the right to access the personal data and the conditions to access such data;
- the use or disclosure of personal data where this is done without the data subject's consent;
- any rejection of a data subject's data subject requests by the data controller, and
- the security measures implemented to protect the personal data.

A Data Processor must maintain a record of all its processing activities in accordance with rules and methods to be eventually prescribed by the PDPC in subsidiary legislation issued under the PDPA.

d) Data Protection Officer ("DPO") and Representative

A DPO will need to be appointed in the following circumstances:

- if the data controller or processor is a public authority as prescribed and announced by the PDPC;

- the activities of the data controller or processor relating to collection, use, or disclosure require regular monitoring of the personal data or the system on a large scale; or

- the core activities of a Data Controller or Processor is the collection, use, or disclosure of sensitive categories of personal data identified in the PDPA.

A data controller or processor must provide the details of the DPO, contact address and contact channels to both the data subject and the PDPC.

Data controllers who are based outside Thailand and subject to territorial scope of the PDPA are required to designate in writing a representative. The representative will need to be based in Thailand and be authorized to act on behalf of the data controller without any limitation of liability with respect to the collection, use or disclosure of personal data by the data controller.

5.9 Security and Data Breach Notification

A data controller must notify the PDPC of any data breach without delay and where feasible, within 72 hours after becoming aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of an individual. Where the breach poses a high risk to the rights and freedoms of individuals, the data breach and remedial measures must also be notified to the data subject without delay.

A data processor must notify the relevant data controller if there is a breach.

5.10 Cross-border Data Transfer

Personal data may not be transferred outside of Thailand unless the recipient country has data protection standards which are commensurate with or better than the PDPA, or where:

- the transfer is for compliance with the law;

- the data subject has given informed consent

- it is necessary for the performance of or entry into a contract to which the data subject is a party;

- it is to prevent or suppress a danger to the life, body or health of the data subject or other individuals.

• it is necessary for carrying out activities in relation to substantial public interest.

Transfers to data controllers or processors within the same affiliated group or group of undertakings are exempt from the above requirements if their data protection policy has been reviewed by the PDPC and certified. Without such certification, suitable protection measures to enable the enforcement of the data subject's rights, including effective legal remedial measures and methods as prescribed and announced by the PDPC, must be implemented.

5.11 Enforcement

Non-compliance with the PDPA may result in administrative fines of up to THB 5,000,000. Criminal breaches of the PDPA may result in fines of up to THB 1,000,000 and/or imprisonment of up to 1 year. Aggrieved data subjects may file civil lawsuits against data controllers and processors, and the court has the power to award up to twice actual damage if judgement is awarded in favor of the data subject.

环球律师事务所 GLOBAL LAW OFFICE SINCE 1979

6. India

6.1 Overview

6.1.1 Legal System

India has a hybrid legal system with elements of civil law, common law, equitable law, and customary & religious laws. It has no specific legislation on data protection. The primary laws dealing with data protection are Sections 43A and 72A of the Information Technology Act, 2000 ("IT Act"), and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("Rules"). The Government of India issued the Personal Data Protection Bill 2019, introduced in the Indian Parliament on 11 December 2019 ("Bill"), which will be India's first specific law on data protection.

6.1.2 Supervisory Authorities

Whilst India possesses a number of regulatory agencies exercising regulatory or supervisory authority over a variety of activities, India does not have a national regulatory authority for protection of personal data. The Ministry of Electronics and Information Technology is responsible for administering the IT Act, and issuing rules and clarifications. The Bill proposes creating a Data Protection Authority of India.

6.1.3 Territorial Scope

The Rules permit both domestic and international data transfers if the recipient ensures the same levels of data protection in India are adhered to, and provided that such transfer is necessary for the performance of a lawful contract between the data collector and the data subject, or has been expressly consented to by the data subject. There are no domestic or cross-border data flow restrictions on information that is not sensitive personal data or information. Similarly, disclosure of sensitive personal data to a third party requires the prior approval of the data subject, unless it has been agreed in a contract or is necessary to comply with a legal obligation. The Rules don't restrict disclosure of non-sensitive personal data. The provisions of the IT Act (except in respect of matters governed by the Rules) are also applicable to any offence committed by a person outside India using a computer, computer system or computer network located in India. The Reserve Bank of India issued a notification on 6 April 2018 making it mandatory for all banks, intermediaries and other third parties, to store all information pertaining to payments data in India. The Bill proposes a new regime for cross-border transfer of personal data and there will be separate requirements for sensitive personal data and critical personal data.

6.1.4 Data Processing Principles

There are no specific principles governing processing of personal data. The Rules require a data collector or any other person possessing information from a data subject on behalf of a body corporate, to possess a privacy policy. The Rules are issued under the IT Act which only applies to electronic records. The Bill proposes a broader application to both physical and electronic records. The data collector is also required to ensure that the policy is available to the data subject, and is published on its website. The privacy policy must describe the type of information collected, the purpose of use of the information, to whom or how the information can be disclosed, and the reasonable security practices and procedures followed to safeguard the information. The privacy policy should also contain details of the grievance officer appointed. The Bill proposes that the processing of personal data will need to comply with seven principles for processing.

6.1.5 Lawful Basis for Processing

A data collector is required to use sensitive personal data only for the purpose for which it was collected, and cannot retain it for longer than is required for the purposes for which the information can lawfully be used, or as otherwise required under any other law.

6.2 Key Definitions

6.2.1 Personal Information

Personal information only affects information about a natural person. Personal data is termed "Personal Information" and is defined under the Rules 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".

6.2.2 Sensitive Personal Data of Information

Sensitive personal data exists under the Rules as personal information which consists of (a) passwords, (b) financial information such as bank account or credit card or debit card or other payment instrument details, (c) physical, physiological and mental health condition, (d) sexual orientation, (e) medical records and history, (f) biometric information, (g) any detail relating to the above items provided to a body corporate for providing services, and (h) any of the information received under the above items by a body corporate for processing, that is stored or processed under lawful contract or otherwise. It does not include information that is freely available or accessible in the public domain or furnished under the Right to Information Act, 2005 or other applicable law. The Bill proposes a broad definition of sensitive personal data and will include financial data, data about caste, tribe, religious and political belief, or affiliation.

6.2.3 Controller and Processor

Indian law does not contain the concepts of controller and processor. The Rules refer to the concept of a body corporate and a provider of information. A body corporate is defined as "any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities". A provider of information is the natural person who provides sensitive personal data or information to a body corporate. The Bill proposes the concepts of a 'data fiduciary' and a 'data processor' equivalent to the concept under the GDPR.

6.3 Data Subject Rights

The data collector is required to take reasonable steps to ensure that the data subject has knowledge of (a) the fact that the information is being collected, (b) the purpose for which the information is being collected, (c) intended recipients of information, and (d) name and address of agency that is collecting the information and the agency that will retain the information. For the collection of sensitive personal data, a data collector is required to obtain the prior written consent from the data subject (which the data subject may refuse to provide). There are no specific formalities to obtain consent for processing personal information. Electronic consent is sufficient. Sensitive personal data must only be collected for a lawful purpose connected with an integral activity of the data collector which is necessary for successfully carrying out that integral activity, and written consent from the provider should be obtained. Consent is not required for personal information which is not sensitive personal data. Data subjects may request a review of the information they provide, and request that inaccurate or deficient information be corrected. Data subjects may withdraw consent at any time. The "right to be forgotten" is not recognized in India. However, Indian courts have recognized this right in relation to sexual offences against women. The Bill proposes a right to be forgotten.

6.4 Privacy Policy and Accountability

A data collector is required to possess and make available a privacy policy. The policy should protect the information that is provided and the provider should be able to review the policy. The policy is required to be made available on the website of the body corporate and should provide for (a) clear and accessible statements relating to its practices and policies, (b) the type of personal information or sensitive personal data or information that is being collected, (c) the purpose of collecting and using of such information, (d) the instances in which disclosure of such information may be made under the Rules, and (e) reasonable security practices and procedures required under the Rules. A privacy policy is required even if no sensitive personal data or information is being processed. The Bill proposes that data fiduciaries take a number of measures to ensure transparency and accountability, including adopting "privacy by design", maintaining transparency regarding its general practices on

processing of personal data, implementing appropriate security safeguards and implementing procedures and mechanisms to address grievance of data principals. The grievance officer shall address any discrepancies or grievances of providers of information with respect to processing of information in a time-bound manner. The grievance officer is required to redress the grievance expeditiously within one month from the date of receipt of such grievance. The body corporate is required to publish the name and contact details of the grievance officer on its website. Whilst the Rules require the appointment of a grievance officer, there is no general requirement to appoint a data protection officer. The Bill proposes that a significant data fiduciary must appoint a data protection officer. In respect to privacy impact assessments, the Rules require those handling and processing sensitive personal data to have their security practices and procedures certified and audited by an independent auditor, who is approved by the central government, at least once every year, or when there is a significant upgrade in its computer resource. There are no rights to data portability.

6.5 Direct Marketing

The IT Act and Rules do not impose any conditions regarding the use of sensitive personal data or information for direct marketing. However, if information is collected from a provider of information (where sensitive personal data or information is collected), the prior consent of the provider must be obtained, including the purpose for which the information is being collected. Apart from the Telecom Commercial Communications Customer Preference Regulations, 2018 issued by the Telephone Regulatory Authority of India to telecom service providers to set up a mechanism to register requests of subscribers not to receive unsolicited commercial calls, there are no specific laws or regulations in India on the use of direct marketing. There are no specific laws or regulations in India on direct marketing by email.

6.6 Children's Privacy Protection

The Rules do not contain any specific rules when processing personal data about children. The Bill proposes that the personal data of a child should be processed so that the rights and the best interests of the child are protected. Such processing can be done only after verifying the age of the child and obtaining consent from the parent or guardian. Entities which process the personal data of children, or provide services directed at children will be categorized as 'guardian' data fiduciaries and will be prohibited from profiling, tracking, or processing the data such that it may cause significant harm to the child.

6.7 Security and Data Breach Notification

Certain types of cybersecurity, incidents need to be mandatorily reported to the Indian Computer Emergency Response Team ("CERT-In") created under Section 70B of the IT Act. These incidents include (a) compromise of critical systems or information, (b) targeted scanning or probing of critical networks and systems, (c) identity thefts, spoofing or phishing

attacks, (d) unauthorized access of IT systems or data, (e) defacement of a website or intrusion into a website, (f) malicious code attacks including attacks on servers, and (g) Denial of Service or Distributed Denial of Service attacks. CERT-In is also authorized to collect or analyses information in relation to cybersecurity, incidents from individuals and organizations. Information that may lead to identification of individuals or organizations that have been affected by cybersecurity, incidents cannot be disclosed without written consent, or through a court order. There is no additional requirement to notify or obtain the approval of any regulatory authority. The Rules provide that reasonable security practices and procedures need to be maintained. A body corporate or a person acting on its behalf is "considered to have complied with reasonable security practices and procedures if they have implemented such security practices and standards and have a comprehensive documented information security program and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business". The Ministry has listed the International Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System -Requirements" as one such standard. Body corporates following other standards are required to get their security practice and standards notified to and approved by the Ministry for effective implementation. A body corporate is required to have its security practice and procedures certified and audited by an independent auditor who is approved by the central government at least once every year, or when there is a significant upgrade in its computer resource. Data protection is generally governed by the contractual relationship between the parties, and the parties are free to agree on their own rules relating to reasonable security practices and procedures, provided the minimum requirements prescribed under the IT Act and the Privacy Rules are met.

6.8 Enforcement

There are no enforcement provisions in relation to data protection in the IT Act or the Rules.

6.9 Miscellaneous

a) Agents: There are no rules that govern third party agents acting on behalf of a body corporate. They are governed by the same regime applicable to body corporates.

b) Fines: Section 72A of the IT Act provides for a fine of up to INR 500,000 when there is a disclosure of personal information in breach of a lawful contract or without consent. The Bill proposes penalties linked to worldwide turnover – ranging from 2% to 4% of the worldwide turnover, depending on the type of breach.

c) Crime: Section 72A of the IT Act provides for imprisonment of up to three years when there is a disclosure of personal information in breach of a lawful contract or without consent.

d) Cookies: There are no specific laws, regulations, or guidelines in India on the use of cookies.

7. The United Arab Emirates (UAE)

7.1 Overview

7.1.1 Legal System

UAE is a federation of seven emirates comprising Abu Dhabi, Dubai, Ajman, Fujairah, Ras Al Khaimah, Sharjah and Umm Al Quwai. The legal system in the UAE is founded upon civil law principles and Islamic Shari'a law. There are federal codes of law which apply in all emirates dealing with fundamental principles of law such as civil, criminal, procedural law and employment law. There are also laws that are specific to each emirate, that are enacted by that emirate's Ruler and relate to matters which are more administrative in nature, such as decrees on the establishment of local authorities, or charities, or amendments to local real estate laws.

In addition, several local emirates have established free zones which have, to varying degrees, their own laws and regulations. The two most important free zones for the purposes of data privacy are the Dubai International Financial Center (DIFC) and the Abu Dhabi Global Market (ADGM). Both are common law jurisdictions and have enacted their own data protection laws and regulations. The free zones are often referred to as offshore while the rest of the UAE is referred to as onshore or mainland.

7.1.2 Supervisory Authorities

• Onshore UAE

There is no general data protection law in onshore UAE and no single national data protection regulator. An individual's right to privacy is enshrined in the UAE Constitution[12], the UAE Penal Code[13], and the Cybersecurity Law.[14] More comprehensive data protection laws apply within the free zones of the DIFC and ADGM. There are also some industry specific laws that impose data related obligations on entities based in mainland UAE and operating within that regulated industry.[15] For example, the UAE's Health Data Law imposes restrictions on the transfer of health information outside of the UAE, unless otherwise prescribed by the concerned federal or local government health authority of the Ministry of Health. The supervisory authority in this instance would be the Ministry of Health and local health authority. It is also worth mentioning that the Telecommunications Regulatory Authority (TRA), and other local agencies tasked with protecting national data and cybersecurity, are looking

12 Article 31 of the Constitution protects the secrecy of an individual's correspondence through the post, telegraph, or other means of communication.

13 Article 378 and 379 of the UAE Penal Code (Federal Law No.3 of 1987) imposes penalties ranging from jail sentences to fines for violating the "private or familial life of individuals", or whoever is entrusted with a secret and divulges it without consent.

14 Article 14 of Federal Decree Law No.5/2010 on Combating Cyber Crimes (Cybercrime Law).

15 See for example Federal Law No.2 of 2019 on the Use of the Information and Communication Technology in Health Fields (Health Data Law) and the Central Bank's Regulatory Framework for Stored Values and Electronic Payment Systems (EPS Regulations).

at implementing a Federal Data Privacy Law. A draft of the law has yet to be made public.

• **DIFC**

On 01 June 2020, the DIFC enacted a new Data Protection Law[16] (DPL) which repeals and replaces Data Protection Law No.1 of 2007 and its related Regulations. The DPL enters into force on 01 July 2020 and entities falling under its scope have a grace period of three months to comply with its provisions. The supervisory authority in the DIFC is the Commissioner of Data Protection.

• **ADGM**

The ADGM adopted Data Protection Regulations in 2015, with amendments introduced in 2018 and 2020.[17] The Office of Data Protection is the supervisory authority in the ADGM responsible for promoting data protection, maintaining the register of data controllers, enforcing the obligations upon data controllers and upholding the rights of individuals.

7.1.3 Material and Territorial Scope

In the absence of a federal data protection law, this section will focus on the material and territorial scope of the DPL and the ADGM DP Regulations.

• **DIFC**

The DPL applies to: (i) the processing of personal data by a controller or processor incorporated in the DIFC, regardless of whether the processing takes place in the DIFC or not; (ii) a controller or processor, regardless of its place of incorporation, that processes personal data in the DIFC as part of stable arrangements, other than on an occasional basis.[18] For the purposes of defining the scope of application of the DPL, "processing in the DIFC" occurs when the means or personnel used to conduct the processing activity are physically located in the DIFC.

• **ADGM**

The ADGM DP Regulations and related Amendments apply to controllers incorporated in ADGM and to processors who process personal data on their behalf.

7.1.4 Data Processing Principles

Since there is no federal data protection law in the UAE, this section will focus on data

16 DIFC Law No. 5 of 2020. Regulations were also issued on 01 July 2020.

17 ADGM Data Protection Regulations 2015 and Amendment Regulations of 2018 and Amendment No.1 Regulations of 2020.

18 Article 6 of the DPL.

processing principles set out in the DPL and the ADGM DP Regulations.

• **DIFC**

The data processing principles set out in the DPL consist of the following: (i) lawfulness, fairness and transparency; (ii) purpose limitation; (iii) data minimization; (iv) compatibility with data subject rights, (v) accuracy; (vi) storage limitation and (vii) integrity and confidentiality.[19]

• **ADGM**

The data processing principles set out in ADGM DP Regulations consist of the following: (i) lawfulness, fairness and security; (ii) purpose limitation in accordance with data subject rights; (iii) data minimization; (iv) accuracy) and (v) storage limitation.[20]

7.1.5 Lawful basis for processing

This section will provide an overview of the requirements for lawful or legitimate processing under the DIFC and ADGM.

• **DIFC**

The bases for processing under the DPL are largely similar to those set out in the GDPR. Processing can be based on consent, contractual necessity, or it might be necessary for the protection of a legal obligation under applicable law, or the protection of a vital interest of a data subject, or for the purpose of legitimate interests pursued by a controller or a third party to whom personal data has been made available, except where such interests are overridden by the interests or rights of a data subject. There are additional bases for lawful processing that apply to specific instances of data processing by a DIFC body.[21]

• **ADGM**

The bases for processing under the ADGM Regulations are similar to those set out in the GDPR. Processing can be based on consent, contractual necessity, compliance with regulatory or legal obligations to which a controller is subject, the protection of a vital interest of a data subject, the performance of a task carried out in the interests of ADGM or one of ADGM's bodies (for e.g. the Court), or for the purpose of legitimate interests pursued by the controller or a third party to whom the personal data are disclosed, provided such interest is not overridden by the compelling legitimate interests of the data subject.[22]

19 Article 9 of the DPL.

20 Article 1 of the ADGM Regulations.

21 Article 10 of the DPL.

22 Article 2 of ADGM Regulations.

7.2 Key Definitions

7.2.1 Personal Data and Special Categories of Personal Data

Personal Data is defined in both the DPL and ADGM Regulations as data referring to an identified or identifiable natural person. Special Categories of Data (referred to as "Sensitive Personal Data" under the ADGM Regulations) are defined as Personal Data revealing or concerning (directly or indirectly) racial or ethnic origin, political opinions, religious or philosophical beliefs, criminal record, trade-union membership and health or sex life. The DPL also includes personal data revealing political affiliation, communal origin and genetic data and biometric data where it is used for the purpose of uniquely identifying a natural person.

7.2.2 Controller and Processor

A controller is defined under the DPL and ADGM Regulations as any person who alone or jointly with others determines the purposes and means of the processing of personal data. Under ADMG Regulations, a controller is a person in ADGM (excluding a natural person acting in his capacity as a staff member).

A processor is defined under the DPL and ADGM Regulations as any person who processes personal data on behalf of a controller. The ADGM Regulations explicitly exclude a natural person acting in his capacity as staff member from this definition.

7.3 Data Subject

The DPL and ADGM Regulations define a data subject as the natural person or, in the case of the DPL the identified or identifiable natural person, to whom personal data relates.

7.4 Privacy Policy

Both the DPL and ADGM Regulations impose an obligation on the controller to provide information to a data subject where personal data has been obtained either directly or indirectly from that data subject. This information should be provided to a data subject as soon as possible at the time of collecting personal data in respect of that data subject, and it can be provided in privacy policies, that are drafted in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Privacy policies should contain information on, for example, the identity and contact details of the controller, the contact details of a DPO, when applicable, the purposes of the processing, the categories of personal data collected, the recipients or categories of recipients of personal data, any information related to transfers to a third country and the

safeguards applied to such transfers, any other information in so far as such is necessary, having regard to the specific circumstances in which the personal data is collected, to guarantee the fair and transparent processing of such data.[23]

7.5 Direct Marketing

The DIFC has issued a specific guidance on direct marketing, which provides information on the requirements that need to be met to undertake such activities.[24] These requirements vary depending on the recipient of the communication and the type of channels used for marketing purposes. ADGM has not issued a similar guidance. The DPL and ADGM Regulations also impose an obligation on controllers to inform data subjects if their data will be used for the purposes of direct marketing, and provide them with the right to object to such use.

7.6 Data Sharing and Processing

ADGM Regulations do not contain specific provisions on data sharing. The DPL however provides instructions to controllers and processors in relation to the disclosure or transfer of personal data following a request from any public authority ("Requesting Authority") over the person or any of its affiliates or its parent company. In case of such requests, the controller or processor should: a) exercise reasonable caution and diligence to determine the validity and proportionality of the request, including to ensure that any disclosure of personal data in such circumstances is made solely for the purpose of meeting the objectives identified in the request from the Requesting Authority; b) assess the impact of the proposed transfer in light of the potential risks to the rights of any affected data subject and, where appropriate, implement measures to minimize such risks; and c) where reasonably practicable, obtain appropriate written and binding assurances from the Requesting Authority that it will respect the rights of data subjects and comply with the general data protection principles set out in the DPL.[25]

7.7 Children's Privacy Protection

There are no provisions related to children's privacy in either the DPL or ADGM Regulations. On a national level, in order to deal with an increase in crimes against children online, the UAE has established various child protection initiatives. A UAE based non-profit organization called e-safe aims to create a safer online experience and to protect children from all types of exploitation.[26] In 2016, a child protection law[27] was also issued by the government. The law obliges telecommunication companies to notify the competent authorities or concerned

23 See Articles 6 and 7 of ADGM Regulations and Article 29 and 30 of the DPL.

24 Commissioner of Data Protection, DIFC Data Protection Policy Guidance: Direct Marketing & Electronic Communications, updated on 01 July 2020 (Guidance).

25 Article 28 of the DPL.

26 http://www.esafesociety.org/en/why-e-safe/

27 Federal Law No. 3 of 2016 on child rights (wadeema's law).

entities of any child pornography being circulated on the internet.[28] Article 5 of this law also provides for a child's right to privacy on the ground of public morals and, while taking into account the rights and responsibilities of the child's custodian.

7.8 Accountability

7.8.1 Data Protection by Design & Default

There are no provisions on data protection by design and default in the ADGM Regulations. The DPL has however introduced this concept in Article 14(3), which imposes an obligation on a controller or processor to integrate necessary measures into the processing of data in order to meet the requirements of this law and protect a data subject's rights. These measures shall at least require assurances that i) processing is designed to reinforce data protection principles such as data minimization at the time of determining the means for processing and at the time of processing itself; and ii) by default, only personal data that is necessary for each specific purpose is processed, and that personal data is not made accessible to an indefinite number of persons without the data subject's intervention.

7.8.2 Data Protection Impact Assessment (DPIA)

The ADGM Regulations do not have any specific provisions on DPIA. The DPL has however introduced an obligation on controller's that undertake high risk processing activities to carry out an assessment of the impact of the proposed processing operations on the protection of personal data, considering the risks to the rights of the data subjects concerned. A controller may also elect to carry out a DPIA in relation to the processing of personal data that is not a high-risk activity. A DPIA shall contain at least: a) a systematic description of the foreseen processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by a controller; b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; c) identification and consideration of the lawful basis for the processing; d) an assessment of the risks to the rights of data subjects; and e) the measures envisaged to address these risks.[29]

7.8.3 Record of Processing Activities

Both ADGM Regulations and the DPL impose an obligation on controllers to establish and maintain written records of personal data processing operations.[30] The DPL also provides that these records shall contain the following information: a) name and contact details of the controller, its appointed DPO, where applicable, and joint controller, if any; b) the purpose(s) of the processing; c) a description of the categories of data subjects; d) a description of

28 Ibid. Article 29.

29 Article 20 of the DPL.

30 Article 12(1) of ADGM Regulations and Article 15 of the DPL.

categories of personal data; e) categories of recipients to whom the personal data has been or will be disclosed, including recipients in third countries and international organizations; f) where applicable, the identification of the third country or international organization that the personal data has or will be transferred to and, the documentation of suitable safeguards in case of transfers to jurisdictions that are not deemed adequate by the Commissioner; g) where possible, the time limits for erasure of the different categories of personal data and h) where possible, a general description of the technical and organizational security measures implemented by the controller.

7.8.4 Data Protection Officer (DPO) and GDPR Representative

ADGM Regulations do not require controllers to designate a DPO. The DPL has however introduced this requirement in Article 16. Both controller and processors may elect to appoint a DPO. A DPO shall also be appointed by DIFC bodies, other than the courts acting in their judicial capacity; and a controller or processor performing high risk processing activities. The DPL provides further information on the competencies and status of the DPO, as well as his role and tasks.[31]

7.9 Security and Data Breach Notification

Article 9(4) of ADGM Regulations imposes an obligation on a processor to inform a controller, as soon as reasonably practicable, of any unauthorized intrusion (including any loss of devices containing personal data or unauthorized disclosures), whether physical, electronic or otherwise, to any personal data held by the processor. A controller also has an obligation to inform the supervisory authority of an authorized intrusion (including any loss of devices containing personal data or unauthorized disclosures) whether physical, electronic or otherwise, to any personal data, including by any of its data processors. Such notification shall be made without undue delay and, where feasible, not later than 72 hours from the time the controller became aware of the incident.

The DPL sets out data breach notification requirements on controllers and processors.[32] A controller shall notify the Commissioner of a personal data breach that compromises a data subject's confidentiality, security or privacy. Such notification shall be made as soon as practicable in the circumstances. A processor shall notify a relevant controller without undue delay after becoming aware of a personal data breach. The DPL also imposes an obligation on controllers to notify data subjects, as soon as practicable in the circumstances, of a personal data breach that is likely to result in a high risk to the security or rights of a data subject. If there is an immediate risk of damage to the data subject, the controller shall promptly communicate with the affected data subject. Where a communication to the individual data subject will involve a disproportionate effort, a controller can issue a public communication

31 See Article 17 and 18 of the DPL.

32 See articles 41 and 42 of the DPL.

or take a similar measure to inform the data subject in an equally effective manner.

7.10 Cross-border Data Transfer

Transfers of personal data out of the DIFC and ADGM are subject to restrictions.[33] Both the DIFC and ADGM have identified several jurisdictions as providing an adequate level of protection for personal data. Personal data can be transferred to these jurisdictions without the need for additional permits or safeguards. Personal data transfers to a jurisdiction in the absence of an adequate level of protection will have to be subject to additional requirements such as, for example, a permit issued by the supervisory authority in the case of ADGM, or the transfer is made with the written consent of the data subject, or if there is a legally binding agreement in place between the exporter and importer of data. The DPL has also recognized Binding Corporate Rules as an appropriate safeguard for an intragroup transfer of data, and the Commissioner has also adopted standard data protection clauses, largely modelled on the EU Model Clauses.[34]

7.11 Enforcement

The supervisory authorities at ADGM and DIFC both have the authority to impose fines on controllers and processors if they contravene the provisions of the applicable data protection legislation. In the case of ADGM, the fines are capped at USD 25,000.[35] In the DIFC, the Commissioner may impose an administrative fine as high as USD 100,000.[36] The Commissioner may also issue a general fine for a contravention of the DPL by a controller or processor in an amount he considers appropriate and proportionate taking into account the seriousness of the contravention and the risk of actual harm to any relevant data subject.[37]

33 Articles 4 and 5 of ADGM Regulations and Articles 26 and 27 of the DPL.

34 Article 27(2) of the DPL.

35 Article 17(3) of ADGM Regulations.

36 Article 62(2) and Schedule 2 of the DPL.

37 Article 62(3) of the DPL.

8. Kingdom of Saudi Arabia (KSA)

8.1 Overview

8.1.1 Legal System

The legal system in KSA is based on Shari'ah law. Shari'ah law is comprised of a collection of fundamental principles derived from a number of different sources, including the Holy Quran, the Sunnah and the works of Shari'ah scholars. In addition to the Shari'ah, the law in Saudi Arabia is also derived from enacted legislation, which can consist of Royal Orders, Royal Decrees, Council of Ministers Resolutions, Ministerial Resolutions and Ministerial Circulars. All such laws are ultimately subject to, and cannot conflict with, the Shari'ah.

8.1.2 Supervisory Authorities

There is no single law which addresses data privacy/protection in Saudi Arabia and no single national data protection regulator. There are however certain regulations, which although not entirely dedicated to data privacy/protection, contain specific provisions governing the right to privacy and data protection in certain contexts.[38]

8.1.3 Material and Territorial Scope

There is no national data privacy law in Saudi Arabia. Some provisions related to data privacy may have extraterritorial reach such as the provisions in the E-Commerce Law that protect consumer data used by online service providers. This law applies to e-commerce platforms located in KSA and to those who offer goods/services to consumers located in KSA, regardless of their place of incorporation. In other words, online service providers located in the UAE who offer goods or services to consumers in KSA via a website would have to comply with the provisions of the E-Commerce Law.

8.1.4 Data Processing Principles

In the absence of a national data protection law, there are no stated principles in relation to data processing.

8.1.5 Lawful basis for processing

There is no lawful basis for processing set out in a national data protection law. Some sector-specific laws may require consent to process personal data in the KSA. In addition, processing of personal data without consent may in certain circumstances constitute a criminal offence. To determine their specific legal obligations, companies operating in the KSA should review

38 See inter alia, Saudi's Basic Law of Governance (Saudi Arabia Royal Decree No. A90/1992), E-Commerce Law (Saudi Arabia Royal Decree No. M126/2019) and the Telecommunications Act (Saudi Arabia Royal Decree No. M12/2001).

sectoral laws appropriate to their operations and handling of data.

The Internet of Things (IoT) Regulatory Framework (IoT Framework) published by the Communications and Information Technology Commission (CITC) also imposes an obligation on providers of IoT services to comply with "data security, privacy and protection requirements". The Framework goes on to state that IoT providers and implementers must "comply with all the existing or future published laws, regulations and requirements… concerning data management including security, privacy and protection". This is an indication that IoT service providers will be required to comply with generally accepted data protection concepts and principles when a national data protection law is implemented. These principles consist of, among other things, purpose limitation, data minimization and storage limitation.

8.2 Key Definitions

8.2.1 Personal Data and Special Categories of Personal Data

There is no uniform statutory definition of personal data in a data protection law in KSA. Sensitive personal data is also not generally recognized in the laws of KSA, although certain data relating to individuals and families would likely be considered sensitive under Islamic tradition and Shari'ah law.

The type of data regulated depends on the applicable law. For example, the Anti-Cyber Crime Law protects data held in electronic form, including but not limited to bank and credit information. The Telecommunications Act regulates data that identifies individual subscribers; and the content of and other information relating to communications between subscribers. The KSA Healthcare Practice Code protects health information such as data that identifies patients, their health status, and the treatments they receive.

There is also no general classification system for personal data applied under Saudi law. However, under the Cloud Computing Regulatory Framework[39] (CCRF), customer data held or processed by cloud service providers is classified into four levels as follows:

• **Level 1:** non-sensitive customer content, whether individuals or private sector companies, not subject to any sector specific restrictions on data outsourcing;

• **Level 2:** sensitive customer content, whether individuals or private sector companies, not subject to any sector specific restrictions on data outsourcing;

• **Level 3:** any customer content from private sector-regulated industries subject to a level categorization via sector specific rules or a regulatory authority decision; and sensitive customer content from public authorities; and

39 Article 3.3.1 of the Cloud Computing Regulatory Framework

• **Level 4:** highly sensitive or secret customer content belonging to a relevant governmental agency or institution.

The CCRF also requires cloud services providers operating in the KSA to apply default levels of security to customer data, which vary depending on the data's sensitivity.

8.2.2 Controller and Processor

There is no concept of data controller or data processor in KSA law.

8.3 Data Subject Rights

There are currently no laws or regulations in KSA setting out specific data subject rights. The only data subject right that can be derived from KSA laws is a general right to privacy and the right to enforce it in court. There is also a requirement in the CCRF for cloud service providers to grant customers the right to delete their data.

8.4 Privacy Policy

The CCRF mandates the provision of certain pre-contract information to cloud customers, such as details of the cloud service provider's data processing activities. There are no other requirements in local law in relation to the information that would have to be provided to a data subject in a privacy policy.

8.5 Direct Marketing

There are no specific rules on the use of personal data for marketing. However, as a general rule, the individual's consent is required for the use or collection of their personal data for any purpose, and for its distribution to third parties.

8.6 Data Sharing and Processing

There are no specific requirements on data sharing in national laws. Foreign requests for the disclosure of data much be made under a bilateral mutual legal assistance treaty (MLAT) and/or a UN convention to which both Saudi Arabia and the requesting state are members. The Ministry of Interior has been designated as the Central Authority for Saudi Arabia for all MLATs signed between Saudi Arabia and its treaty partners.

8.7 Children's Privacy Protection

The Child Protection Law 1436H and the Regulations for the Child Protection System provide the legal framework for the protection of children in KSA. The law contains general provisions

on the rights of children. It does not however contain any specific provisions related to children's right to privacy.

8.8 Accountability

a) Data Protection by Design & Default

There is no such requirement under Saudi national laws.

b) Data Protection Impact Assessment (DPIA)

There is no requirement to undertake a DPIA under Saudi national laws.

c) Record of Processing Activities

There is no requirement to keep a record of processing activities under Saudi national laws.

d) Data Protection Officer (DPO) and GDPR Representative

Entities that collect, use or process personal data are not currently required to designate a DPO under Saudi national laws.

8.9 Security and Data Breach Notification

Since there is no national data supervisory authority in KSA, there is currently no obligation to report data breaches, except for breaches affecting cloud service providers (CSP). Under the CCRF, a CSP must inform its customers, without undue delay, of any security breach or information leakage that those CSPs become aware of, if such breach or leakage affects, or is likely to affect, these customers' cloud content, their data or any cloud service they receive from that CSP. The CSPs must also inform the Communication and Information Technology Commission (Commission), without undue delay of any security breach or information leakage that they become aware of, if such breaches or data leakages affect, or a likely to affect: a) any level 3 customer content; b) the customer content or data of a significant number of customers; c) a significant number of persons in KSA because of their reliance on one or more cloud customers' services that are affected by the security breach or information leakage.

While the CCRF does not set out fines for data breaches, there are fines under the KSA Anti-Cybercrime Law for perpetrators of such data breaches. The Anti-Cybercrime Law punishes any person that illegally: i) accesses the computer of another for the purpose of deleting, destroying, altering, or redistributing its information by a fine not exceeding 3,000,000 Saudi Riyals (approximately USD 800,000) and/or imprisonment for a period not exceeding four years; ii) accesses the bank or credit information of another or information pertaining to its

owned securities by a fine not exceeding 2,000,000 Saudi Riyals (approximately US$ 533,333) and/or imprisonment for a period not exceeding three years; iii) interrupts data that is transmitted through a computer or an information network by a fine not exceeding 500,000 Saudi Riyals (approximately US$ 133,333) and/or imprisonment for a period not exceeding one year.

8.10 Cross-border Data Transfer

The CCRF imposes restrictions on the transfer and location of data depending on its classification. For example, level 3 customer data may not be transferred outside of KSA, for whatever purpose and in whatever format, whether permanently or temporarily (e.g. for redundancy or caching), unless this is expressly allowed under the laws or regulations of KSA, other than the CCRF.

Aside from localization requirements for certain types of data under the CCRF, or other applicable laws, there are no agreed upon mechanisms for the transfer of data. No standard form or precedent data transfer agreements, such as Standard Contractual Clauses, have been approved by the national authorities of Saudi Arabia. This situation is anticipated to change when a national data protection law is adopted. In the meantime, it is advisable to obtain the consent of a data subject prior to any export of their personal data to avoid a breach of general Sharī'a principles.

8.11 Enforcement

There is no clear supervisory authority responsible for the enforcement of data protection and privacy. That said, specific authorities are tasked with enforcing breaches of other legislation that is in place in the KSA. Penalties for violating data protection and data privacy are either set out in related regulations or left to the judge's discretion. Section ix above outlines some of the sanctions imposed under the Anti-Cyber Crimes Law. Individuals whose right to privacy has been infringed may also have recourse under Shari'ah law and be eligible for compensation if they suffer a loss as a result of their information being disclosed to a third party. The third party who has illegally or unethically obtained the data will be liable for such disclosure.

IV. Oceania

1. Australia

1.1 Overview

1.1.1 Legal System

The Commonwealth Privacy Act 1988 (Privacy Act) is the main privacy legislation. There is separate Commonwealth legislation that governs spam and telemarketing, and telecommunications-specific privacy legislation. There are also a number of binding Codes, Rules and Guidelines in relation to specific areas (such as medical research, tax file numbers, credit reporting, and Commonwealth government agency governance). Each state and territory also have legislation that governs the collection and use of information obtained through surveillance, and the states and territories have separate privacy legislation that regulates government bodies in that jurisdiction. Some states and territories have separate legislation in relation to health records.

1.1.2 Supervisory Authorities

The Office of the Australian Information Commissioner (OAIC) oversees and enforces the Privacy Act.

1.1.3 Material and Territorial Scope

The Privacy Act applies to any Australian federal department or body (agency) and all private organizations with an annual turnover exceeding AUD $3 million (organizations). Agencies and organizations are together referred to as entities. The Privacy Act also applies to small businesses below the AUD $3 million threshold that meet certain criteria (for example are health service providers, that deal in personal information, are a contracted service provider for a commonwealth contract, are credit reporting bodies, are part of a larger corporate group (where one or more members exceeds the AUD $3 million threshold), are required to comply with anti-money laundering obligations, or are subject to the telecommunications mandatory data retention scheme).

The Privacy Act has extra-territorial application and applies to any foreign entity that carries on business in Australia and collects or holds information in Australia.

The Privacy Act does not apply to employee records, being a record of personal information relating to the employment of the employee (such as engagement, training, discipline, performance, personal contact details, wages, leave entitlements, or tax and banking affairs) that is directly related to a current or former employment relationship between the

employer and individual.

1.1.4 Data Processing Principles

The Privacy Act establishes the 13 Australian Privacy Principles (APPs) which govern the way personal information is collected, used, disclosed, and stored. The APPs address open and transparent management of information, anonymity and pseudonymity, collection use and disclosure, direct marketing (but with limited application), overseas disclosure, government identifiers, quality and security, access, and correction.

1.1.5 Lawful basis for processing – APP 3

An entity must not collect information unless it is reasonably necessary for one or more of its functions or activities, and must only do so by lawful and fair means. An entity must not collect sensitive information unless the individual expressly or impliedly consents to the collection, and the information is reasonably necessary for one or more of its functions or activities.

1.2 Key Definitions

a) **Personal information -** means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not.

b) **Sensitive information -** means information or an opinion about an individual's racial or ethnic origin, political opinions or membership; religious or philosophical beliefs or affiliations, membership of a trade union or professional or trade association, sexual orientation or practices, criminal record, health or genetic information, biometric information for automated biometric verification or identification, or biometric templates.

c) **Controller and Processor -** instead of the concepts of data controllers or processors the Privacy Act refers to the collection, use and disclosure of personal information, and applies to all entities captured by the Privacy Act.

1.3 Data Subject Rights

• Access – APP 12

An individual has the right to access their information held by an entity. The entity must make the information available to the individual within a reasonable period (usually 30 days) unless limited exceptions apply. Organizations (but not agencies) can charge for access.

• **Correction – APP 13**

Entities must correct personal information if requested by the individual to whom the information relates, or the information is inaccurate, out of date, incomplete, irrelevant, or misleading. In some cases, entities must notify the correction to other entities who have the same information. APP entities can refuse to correct information in limited circumstances. Organizations (but not agencies) can charge for access.

1.4 Privacy Policy

Entities must have a clearly expressed and up-to-date privacy policy which includes the details set out under APP 1.4, as well as separate collection notice under APP 5. Many entities only have a single privacy policy that includes both the APP 1.4 and 5.2 requirements – identification and contact details, the type of information collected and the method and purpose of collection (including any Australian laws or orders requiring the collection) and the consequences of non-collection, how the information is used and disclosed (including overseas), how an individual may access and correct their information, and how an individual may complain about privacy practices.

1.5 Direct Marketing

APP 7 only applies to hard copy marketing, or targeted electronic advertising where personal information was collected from the individual, and the individual would reasonably expect it to be used for that purpose. If not collected from the individual, there is no reasonable expectation, or the information is sensitive information, it can only be used for direct marketing with the individual's express or implied consent. Opt-out information must also be provided.

The Spam Act 2003 (Cth) prohibits the sending of unsolicited commercial electronic messages (including email, SMS, and MMS) without express or inferred consent. Messages must also clearly identify the sender and contain a functional unsubscribe facility.

The Do Not Call Register Act 2006 (Cth) and Telecommunications (Telemarketing and Research Calls) Industry Standard 2017 regulate the use of telemarketing.

1.6 Data Sharing and Processing – APP 6

Personal information collected for a particular purpose (the primary purpose), must not be used or disclosed for another purpose (the secondary purpose), unless:

a) the individual has expressly or impliedly consented to the secondary purpose;

b) the individual would reasonably expect it to be used for the secondary purpose, which must be related to the primary purpose (directly related for sensitive information); or

c) there is a permitted general situation, a permitted health situation, it is required by an Australian law or court order, or is necessary to assist an enforcement body.

1.7 Children's Privacy Protection

The OAIC has advised that an individual under 15 does not have the capacity to consent.

1.8 Accountability

a) Data Protection by Design & Default

APP 1 includes similar requirements to the GDPR privacy by design and default principles encouraging the establishment of practices and procedures to help an entity protect personal information and comply with the APPs. APP 1.1 encourages entities to manage personal data in an open and transparent manner. APP 1.2 requires that entities take reasonable steps to implement practices procedures and systems that enable the entity to comply with the APPs.

b) Data Protection Impact Assessment (DPIA)

DPIAs are not mandated for organizations, however agencies will need to undertake DPIAs where directed to do so by the OAIC or under the Australian Government Agencies Privacy Code 2017.

c) Record of Processing Activities

Not required.

d) Data Protection Officer (DPO) and Representative

Not required.

1.9 Security and Data Breach Notification

Under APP 11, entities must take such steps as are reasonable in the circumstances to protect personal information from misuse, interference, and loss, and from unauthorized access, modification, or disclosure. Entities must also take reasonable steps to destroy or de-identify personal information once it is no longer required for a permitted purpose.

Entities must investigate a data breach to assess whether or not it is notifiable within

30 days of becoming aware of the data breach. A notifiable data breach occurs where a reasonable person would consider that the loss or unauthorized access or disclosure is likely to cause serious harm to the affected individual. Entities must notify both the OAIC and affected individuals of a notifiable data breach, and the notification must include mandated information.

1.10 Cross-border Data Transfer – APP 8

Before disclosing personal information overseas, entities must enter into written agreements with overseas recipients requiring them to comply with the APPs. The disclosing entity is ultimately responsible for the overseas recipient's compliance with the APPs. These requirements do not apply where:

a) the overseas recipient is subject to a similar law or binding scheme as the APPs;

b) the individual is expressly informed the entity won't take steps to ensure the overseas recipient complies with the APPs, and the individual provides the information after so being informed; or

c) disclosure is required or authorized under an Australian law or court order, or there is a permitted general situation.

1.11 Enforcement

The OAIC can issue determinations (with penalties of up to AU$20,000 to date), enforceable undertakings, or seek civil penalty orders of up to AU$420,000 or pecuniary penalty orders of up to AU$2.1 million.

1.12 Upcoming Changes to Legislation

In July 2019, the Australian Competition and Consumer Commission released a report on its inquiry into digital platforms. This Guide made a number of recommendations for existing legislation including a number of recommendations for strengthening the protection of personal information under the Privacy Act, a number of which the government has committed to implementing, likely in 2021. These include:

a) increasing penalties to the greater of (i) AUD $10 million (ii) three times the value of the benefit obtained through the misuse of information and (iii) 10% of the entity's annual turnover;

b) expanding the definition of personal information and the scope of the Privacy Act;

c) strengthening notice and consent requirements;

d) introducing a direct right of action for individuals, including considering the introduction of a tort of privacy; and

e) developing a binding privacy code for social media and online platforms.

环球律师事务所 GLOBAL LAW OFFICE SINCE 1979
环球律师事务所 GLOBAL LAW OFFICE SINCE 1979

2. New Zealand

2.1 Overview

2.1.1 Legal System

New Zealand has the Privacy Act 1993 (Privacy Act). Additional protections are provided by Codes of Practice including the Health Information Privacy Code 1994, the Credit Reporting Privacy Code 2004, and the Telecommunications Information Privacy Code 2003.

2.1.2 Supervisory Authorities

The Office of the Privacy Commissioner (OPC) oversees the Privacy Act. Binding decisions in relation to the Privacy Act are made by the Human Rights Review Tribunal.

2.1.3 Material and Territorial Scope

The Privacy Act applies to any person whether incorporated and unincorporated, and both private and public sector agencies (together refer to as agencies). The OPC has stated that an international agency will be subject to the Privacy Act if it operates in New Zealand and provides services to New Zealanders, despite its data processing taking place overseas.

2.1.4 Data Processing Principles

The Privacy Act establishes 12 Information Privacy Principles (IPPs) which cover collection, storage and security, requests for access to and correction of personal information, accuracy, retention, use and disclosure, and the use of unique identifiers. The Privacy Act also sets out a number of additional requirements in the body of the legislation. IPPs 5 to 8, and IPP 11, specifically apply to information held outside New Zealand.

2.1.5 Lawful basis for processing - IPP 1

Agencies must not collect personal information unless the information is collected for a lawful purpose, connected to a function or activity of the agency, and the collection is necessary for that purpose.

2.2 Key Definitions

2.2.1 Personal Information

Personal Information means information about an identifiable individual; and includes information relating to a death that is maintained by the Registrar General pursuant to the Births, Deaths, Marriages, and Relationships Registration Act 1995, or any former Act.

2.2.2 Controller and Processor

The Privacy Act doesn't refer to controllers or processors, although it does have a concept similar to a processor - information held for the sole purpose of processing on behalf of another agency is considered to be held by that other agency.

2.3 Data Subject Rights

a) Access - IPP 6 and Parts 4 and 5 of the Privacy Act

Where an agency holds readily retrievable personal information, upon request it must confirm whether it holds such information, and provide access to that information within 20 working days of the request.

b) Correction - IPP 7 and Parts 4 and 5 of the Act

Agencies must, upon request or on their own initiative, take such steps as are reasonable in the circumstances (and subject to a number of permitted exceptions) to correct information (within 20 working days) to ensure it is accurate, up to date, complete, and not misleading. having regard to the purposes for which the information may be used. In some cases, agencies must notify the correction to other entities who have the same.

2.4 Privacy Policy

There is no specific requirement for an agency to have a privacy policy however IPP 3 sets out a number of details of which agencies must make consumers aware, including; that the information is being collected, the purpose of collection, the intended recipient(s), the name and address of the agency collecting and holding the information, if the collection is required or authorized under law, the consequences if the information is not provided, and the rights of access and correction provided by the IPPs.

2.5 Direct Marketing

The Privacy Act doesn't contain any specific requirements in relation to direct marketing; however, it does apply the general concepts set out in the IPPs, such as transparent use of information and authorization by the individual.

The 2007 Unsolicited Electronic Messages Act prohibits the sending of commercial electronic messages (CEMs) without the recipient's inferred or express consent. The CEM must also clearly identify the sender and contain a functional unsubscribe facility.

The Marketing Association of New Zealand maintains the Do Not Call and the Do Not Mail

Registers which regulate the use of telemarketing and physical mailing. The Association also administers a number of codes of practice and guidelines that apply to direct marketing. While these codes are voluntary, they are endorsed by the New Zealand government and compliance is expected.

2.6 Data Sharing and Processing – IPP 10

An agency that collects information for one purpose must not use it for any other purpose unless the information is publicly available and it would not be unfair or unreasonable to use the information, the other purposes or use is authorized by the individual, where non-compliance is necessary to avoid prejudice to the maintenance of the law by any public sector agency or the enforcement of a law imposing a pecuniary penalty, protection of the public revenue or for the conduct of proceedings, the use of the information is necessary to prevent or lessen a serious threat to public health or safety or the life or health of an individual, the other purpose is directly related to the initial purpose, the information is used in a form in which the individual is not identified, or where a specific exemption to IPP 10 is granted by the OPC.

2.7 Children's Privacy Protection

The Privacy Act doesn't treat children's information differently allowing children the same rights as adults when dealing with their information. The OPC has nonetheless recommended that agencies take a practical approach and treat the child's parents or guardians as the child's representatives when dealing with very young children.

The Privacy Act makes some allowances for the refusal of access requests in the case of a child where allowing access may endanger the safety of any individual, or where disclosure in the case of an individual under the age of 16 would be contrary to that individual's interests.

2.8 Accountability

a) Data Protection by Design & Default

There are no express provisions requiring privacy by design and default, other than the general principles set out in the IPPs.

b) Data Protection Impact Assessment (DPIA)

DPIAs are not mandatory under the Privacy Act however the OPC encourages the use of DPIAs where a project may impact personal information and the reasonable expectations of privacy.

c) Record of Processing Activities

Not required.

d) Data Protection Officer (DPO)

Agencies are required to have one or more individuals responsible for the encouragement of compliance with the IPPs, dealing with requests made pursuant to the act, working with the commission in relation to an investigation and otherwise ensuring compliance by the agency. There are no registration requirements.

2.9 Security and Data Breach Notification – IPP 9

Agencies must not keep information for longer than is required for the purposes for which the information may lawfully be used.

It is not compulsory to report a data breach however the OPC has released non-binding best practice guidelines in the event of a breach.

2.10 Cross-border Data Transfer

The Privacy Act does not have any specific restrictions on the cross-border transfer of personal information, but does provide that agencies that transfer information outside New Zealand will remain responsible for the overseas recipient's use and disclosure of the information.

The OPC may prohibit the international transfer of personal information if it is satisfied that information received in New Zealand from an overseas country is likely to be transferred to another overseas country which doesn't have privacy protections similar to those in New Zealand, and the transfer would likely breach the data protection obligations of the OECD Guidelines.

2.11 Enforcement

The OPC has limited enforcement powers – it can assess complaints and compel agencies to meet with the affected individual to attempt to reach an agreed settlement. The OPC may also issue fines of up to NZ $2000 for failure to comply with the OPC's investigations.

The OPC may refer any complaints where the agency and individuals have failed to reach a settlement to the Human Rights Review Tribunal, which can issue fines which vary depending on the severity of the breach. Fines may range from NZ $5,000 to NZ $10,000 for less serious cases, and from NZ $50,000 upwards for more serious cases.

2.12 Upcoming Changes to Legislation

The Privacy Act 2020, which comes into effect on 1 December 2020, substantially re-writes the current legislation.

- Key reforms include:
- mandatory data breach reporting;
- introduction of compliance notices;
- the OPC having powers to make binding decisions;
- increased cross-border data transfer protections;
- making it a criminal offence to mislead an agency in a way that affects another individual's information, and to destroy documents when an access request has been; and
- strengthening of the OPC's information gathering powers, with fines for non-compliance with an investigation increased to NZ $10,000.

环球律师事务所 GLOBAL LAW OFFICE SINCE 1979

Part IV
Legal Framework for Cross-border Data flow

I. European Union

Under the GDPR, transfers of EEA originating personal data to third countries outside the EEA are not permitted unless done pursuant to:

- European Commission adequacy decision: The list of countries which have been approved by the European Commission includes Andorra, Argentina, Canada (where PIPEDA applies), the USA (for organizations participating in the EU-US Privacy Shield), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, Eastern Republic of Uruguay and New Zealand;[40]

- Standard Contractual Clauses ("SCCs"): either adopted by the European Commission or adopted by a DPA and approved by the European Commission;

- Binding Corporate Rules ("BCRs") approved by the competent DPAs; or

- Derogations (e.g. explicit consent, contractual necessity, public interest, legal claims, etc.) or specific exemptions. (Art.44-50, GDPR)

40 The USA (for organizations participating in the EU-US Privacy Shield) was regarded as one of the countries obtaining the adequacy decision. However, the CJEU judgement on 16th July 2020 invalidated the EU-US Privacy Shield, and thus organizations can no longer rely on this mechanism for data transfer.

Ⅱ. Multilateral Framework

1. CPTPP Framework

The Comprehensive and Progressive Agreement for Trans-Pacific Partnership ("CPTPP"), formerly known as the Trans-Pacific Partnership ("TPP") is a free trade agreement between the following 11 participating economies: Australia, Brunei Darussalam, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, and Vietnam.

Articles 14.11 and 14.13 of the CPTPP set out a number of rules which are intended to restrict the imposition of data localization and requirements on cross-border transfers of data by participating economies:

Article 14.11 requires the participating economies to "allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of business"; and

Article 14.13 prohibits a participating economy from requiring a company to "use or locate computing facilities in that Party's territory as a condition for conducting business in that territory."

(collectively, the "Freedom of Transfer Provisions")[41].

The Freedom of Transfer Provisions reflect the participating economies' commitment to facilitating the free flow of data across borders, and are expected to impact the national rules applicable to cross-border transfers of data in these countries.

2. CBPR for APEC Countries

The Asia-Pacific Economic Cooperation ("APEC") Cross-Border Privacy Rules ("CBPR") is a government-backed data privacy certification that companies can join to demonstrate compliance with internationally-recognized data protection provisions. CBPR-certified entities are deemed to comply with applicable cross-border data transfer requirements when it transfers or receives personal data across participating CBPR economies. There are currently 9 participating APEC economies in the CBPR system: USA, Mexico, Japan, Canada, Singapore, South Korea, Australia, Taiwan (China) and the Philippines.

41 It should be noted that the Freedom of Transfer Provisions are subject to a number of carve-outs within the CPTPP. For instance, the provisions do not prevent a participating economy from adopting or maintaining data localisation measures in pursuit of a "legitimate policy objective" (see paragraph 3 of Articles 14.11 and 14.13 of the CPTPP). The provisions also do not apply to data related to government procurements, government information and financial institutions (see Article 14.1 and paragraph 3 of Article 14.2).

In order to be CBPR-certified, companies will need to be assessed against an assessment framework ("CBPR Program Requirements") which is based on the APEC Privacy Framework and features 9 privacy principles: Accountability, Prevent Harm, Notice, Choice, Collection Limitation, Use of Personal Information, Integrity of Personal Information, Security Safeguards and Access and Correction. Examples of the criteria used to assess companies under the CBPR Program Requirements include the accessibility and comprehensiveness of the company's privacy policies, the degree of transparency in relation to choices regarding data collection and consent, as well as the measures implemented and standards to which personal data is retained and protected.

环球律师事务所 GLOBAL LAW OFFICE SINCE 1979
环球律师事务所 GLOBAL LAW OFFICE SINCE 1979

环球律师事务所
GLOBAL LAW OFFICE
SINCE 1979
环球律师事务所
GLOBAL LAW OFFICE
SINCE 1979

环球律师事务所 GLOBAL LAW OFFICE SINCE 1979

Wolters Kluwer
荷兰威科集团

Wolters Kluwer is a leading global information services and solutions company. It provides information, software, and services that help legal, tax, finance, and healthcare professionals make their most critical decisions effectively and with confidence. Customers depend on Wolters Kluwer services and solutions to successfully move through the complex layers of data and regulation that define modern business and government.

Wolters Kluwer entered Mainland China in 1985. Depending on global connections and experience as well as dedication to local markets and client needs, Wolters Kluwer is able to provide timely, accurate and authoritative information solutions to Chinese professionals in legal, tax and accounting, finance and healthcare fields.

Wolters Kluwer employs nearly 19,000 people worldwide with the revenue reached 4.61 billion euros in 2019. It is headquartered in Alphen aan den Rijn, the Netherlands and has offices in Europe, North America, Asia Pacific and Latin America to support clients' needs globally. Wolters Kluwer shares are listed on NYSE Euronext Amsterdam (symbol: WKL) and are included in the AEX and Euronext 100 indices.

环球律师事务所 GLOBAL LAW OFFICE SINCE 1979
环球律师事务所 GLOBAL LAW OFFICE SINCE 1979