STUDIES IN PRIVATE INTERNATIONAL LAW - ASIA

PRIVACY AND PERSONAL DATA PROTECTION LAW IN ASIA

Edited by Adrian Mak,
Ching Him Ho and Anselmo Reyes

CONTENTS

LIST OF CONTRIBUTORS

Adam Au is general counsel at Toys R Us Asia.

Khin Thitsar Aung is an Associate Professor in the Department of Law at Yangon University of Distance Education.

Eng Yi Chia is an Associate at Cecil Abraham & Partners in Malaysia.

Eung-Kyung Cho is an Attorney-at-Law in South Korea.

Sai Ramani Garimella is an Associate Professor at South Asian University in India.

Lanx Goh is Global Head of Privacy at Prudential Plc, Adjunct Associate Professor at the National University of Singapore, Adjunct Lecturer at the Singapore Management University, and Honorary Consul of the Republic of Bulgaria in Singapore.

Ching Him Ho is a barrister at Plowman Chambers in Hong Kong.

Abdulaziz Jurajonov is an Associate (Advocate) at Centil in Uzbekistan.

Joshua Kow is Corporate Counsel (Privacy & Data) at Sony Interactive Entertainment.

Mai-Thanh Le is a Professor at Thang Long University in Hanoi, Vietnam.

Lemuel Didulo Lopez is a Lecturer at RMIT University in Australia.

Adrian Mak is a Mediator based in Hong Kong and a Director of Kabishiki Kaisha Anselmo Reyes in Japan.

Haaris Moosa is an Advocate of the High Court of Kerala in Kochi, India.

Abdumalik Mukhtorov is an Advocate at Azizov & Partners in Uzbekistan.

Rothna Ngorn is a Senior Associate at Bun & Associates in Cambodia.

Tien-Duc Nguyen is a Research Fellow at the Institute of State and Law of the Vietnam Academy of Social Sciences.

Botagoz Omarova is a lawyer at Azizov & Partners and a Leading Researcher at the Institute of Legislation and Legal Information of the Ministry of Justice in Kazakhstan.

Priskila Pratita Penasthika is an Assistant Professor at the Faculty of Law of Universitas Indonesia.

Hemaka Perera is an Associate Counsel (Foreign) working with VK Rajah SC in Singapore.

Anselmo Reyes is an International Judge of the Singapore International Commercial Court.

Nobuyuki Sato is a Professor at Chuo Law School and Executive Vice-President of Chuo University.

Introduction

CHING HIM HO AND ANSELMO REYES

I. Overview

This chapter has several objectives. Its overall purpose is to introduce data privacy and protection law to readers who are unfamiliar with the subject. Section II will seek to justify the inclusion of a book on Asian data protection regulations in a series devoted to the conflict of laws in Asia. Section III is an initial attempt at identifying trends in the data protection regulations of Asian states. It will be suggested that a key trend is for Asian states to be influenced, to a greater or lesser extent, by the European Union's (EU) General Data Protection Regulation (better known as GDPR),[1] in the development of their data protection regimes. A more in-depth comparison of Asian data regimes will be found in the Conclusion to this book. The heart of this chapter is to be found in sections IV and V. As not all readers will be familiar with GDPR, section IV will summarise its basic provisions. Section V will then submit that the EU's principles can serve as a template against which to benchmark the 17 data protection regimes surveyed in the succeeding chapters of this book.

II. Data Protection and the Conflict of Laws

This is the fifth thematic volume within the *Studies in Private International Law: Asia* series. The thematic volumes are supposed to be studies of specific conflict of law in Asian jurisdictions. However, in contrast to previous thematic volumes which concentrated on the standard issues of private international law (jurisdiction, applicable law, the enforcement of judgments or awards across state borders, and the harmonisation of cross-border law), this book focuses on how 17 Asian states have sought to safeguard personal data in their domestic law.[2] Accordingly, a large part of this book concerns what might be characterised as purely regulatory law, prompting one to query how this book can purport to be a study of private international law.

We respond to the query by way of an intuitive examination of the notions of 'personal information or data', 'privacy', and 'protection' pervading this book. We suggest that, simply

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (2016) OJ L119/1, available at gdpr-info.eu/.

[2] The Asian states are China, Hong Kong, Taiwan, Japan, South Korea, Singapore, Malaysia, Vietnam, Cambodia, Myanmar, the Philippines, Indonesia, Thailand, Sri Lanka, India, Uzbekistan and Kazakhstan.

on an intuitive level, three issues come straightaway to mind when one considers the notions highlighted.

The first issue is the scope of one's personal information or data. What qualifies as information or data that is personal to a human being (that is, a data subject)? As a matter of principle, every detail about oneself and how one interacts with the world at large should constitute one's personal information or data. On this footing, the ambit of personal information is wide, ranging from matter-of-fact details about a person (name, sex, marital status, address, occupation, nationality, race, birth date, height, weight, and level of education) to more intimate descriptions of one's habits and activities (tastes in music and literature, activities on social media, and spending patterns).

Given such a wide definition of what personal data comprises, the second issue is whether every datum or piece of information about oneself constitutes one's 'privacy'. In other words, to what extent is a data subject entitled to deny access to information about oneself, so that the world at large can only know such information if the individual consents. If not all one's personal data are to be regarded as off-limits in the absence of consent, how is the line to be drawn between what information is (and what information is not) entitled to be treated as private to oneself. What are the underpinning principles for personal information or data to be classified as off-limits to outsiders?

The third issue shifts from an understanding of the nature of personal data and privacy to an examination of regulatory regimes for permitting or denying access to such private data. The accounts of the data protection regimes in the 17 Asian states contained in this book focus on the following matters:

1) When may an individual's private information be:
   a) collected,
   b) processed,
   c) transferred to third parties, or
   d) stored,

   by data controllers and processors?
2) What conditions (if any) govern such collection, processing, transfer, or storage?
3) What remedies (if any) are available to data subjects whose information has been wrongly collected, processed, transferred, or stored?

Even on the intuitive understanding just sketched out, it will be apparent that cross-border issues inevitably arise, especially given the ubiquity of cyberspace and the vast amounts of personal data now being transmitted by individuals to corporations or natural persons over social media and the internet at every second of every day. The three matters identified in the previous paragraph readily give rise to a host of sub-questions which are analogous to the standard topics of private international law. This is because, although a country's data protection regimes purport to regulate the handling of personal information within its boundaries, in practice the regime must be extra-territorial to be effective. Cyberspace knows no territorial limits. It can be accessed from anywhere, so that a state's data protection regime must extend to regulating what is available over the internet anywhere and everywhere in the world.

There are consequently issues of jurisdiction and applicable law: (1) To what extent (if at all) will the data protection laws of state A apply to a data controller or processor in state B who has wrongly collected, processed, transferred, or stored the personal information of a data subject residing in state A?

There are issues of recognition and enforcement beyond a state's boundaries: (2) Suppose that state B has a more stringent regime for the protection of personal data than state A, can a data subject residing in state A invoke the protection of state B's laws against a data controller or processor who has wrongly exploited that individual's personal information? (3) What means (if any) are available to a data protection supervisory authority in state A to enforce state A's data protection laws against a data controller or processor in state B who maintains no (or no substantial presence) in state A? (4) What means (if any) are available to the data protection supervisory authority in state B to ensure that state A does not make unreasonable demands of what should (or should not be done) by state B's data privacy regulatory regime for the protection of the personal information of data subjects residing in state A?

There are issues of conflict and harmonisation: (5) Is the consequence of the answers to the foregoing sub-questions that, in practice, data controllers and processors will have to comply with the totality of data protection laws in the countries in which they operate or in which their services or products may be accessed? (6) What if those data protection laws are inconsistent with each other?

There are policy issues about where we are (or should be) heading with so many overlapping data protection and privacy regimes: (7) With ever-increasing regulation, what has become of notions such as the 'freedom of the internet commons' and 'access to information' that the advent of the web was supposed to usher?

In short, there are an abundance of conflict of law issues, which can only be approached through a study of different regulatory regimes and their interactions with one another.

III. Some Asian Trends

A divergence in how different Asian states categorise and regulate personal data renders the identification of common ground among them difficult. Nonetheless, we submit that the following common characteristics can be discerned.

In 1948, by Article 12 of the Universal Declaration of Human Rights, the UN acknowledged a human right of privacy: 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.'[3] Since then, many states have recognised privacy as a fundamental right, despite uncertainties as to the precise meaning of the concept. Data privacy rights have been enshrined in constitutions, national law, administrative regulations, and case precedents, as a means of safeguarding the individual's right to privacy and the collection, use and transfer of an individual's personal data. Among the Asian jurisdictions studied here, Japan,[4] Hong Kong,[5]

[3] UN, Universal Declaration of Human Rights (1948), available at un.org/en/about-us/universal-declaration-of-human-rights.
[4] Constitution of Japan, Art 13.
[5] Hong Kong Basic Law, Art 30.

South Korea,[6] Myanmar,[7] Kazakhstan,[8] Vietnam,[9] and Thailand[10] have expressly identified privacy as a fundamental right in their constitutional documents. Other states (such as Sri Lanka,[11] Taiwan,[12] Cambodia,[13] Singapore,[14] and Indonesia[15]) have not explicitly referred in their constitutions to a person's right to privacy, but have acknowledged the right to privacy as a fundamental human right in their legislation or court decisions.

Among the 17 jurisdictions covered in this volume, most have enacted a data protection legal framework, with Myanmar and Cambodia being the exceptions. In general, data protection in such frameworks refer to protection against the unwanted disclosure of personal information.[16] Thus, doxing (that is, disclosure of others' personal data without consent) is typically criminalised. Among Asian states where data protection laws are in place, the relevant regimes mirror GDPR to a greater or lesser extent. Most states' legislation broadly prohibits the transfer of personal data from their jurisdiction to states which do not have data protection regulations affording a similar standard of protection.

Nonetheless, differences exist. Individual states have included special features in their data protection laws. In Taiwan, for instance, the restriction on international transfer of personal data applies only to non-public entities. The Personal Data Protection Acts of Singapore and Indonesia[17] exclude liability in the case of an individual acting in a personal or domestic capacity, or when the data concerned comprise 'business contact information'.[18] Hong Kong has a 'whitelist' regulation (that is, a requirement that data only be transferred to states having a similar level of protection). However, that has not yet come into operation, apparently due to a lack of consensus on the matter among the business community.[19] Consequently, although GDPR has provided the backbone for data protection regimes in Asia, each state has modified GDPR, adapting it to local circumstances and needs.

An individual's privacy and personal data may be governed by different sets of legislation within a state. One set of laws will deal with an individual's rights as a human being, highlighting paradigm situations of privacy violation and providing for compensation or some other remedy in case of infringement. A different set of laws will govern what others (natural or legal persons) can do with an individual's personal data, in particular regulating the collection, processing, transfer and storage of personal data. For instance, in Taiwan the right to privacy is regulated by the Civil Code, whereas the protection of personal data is covered by the Personal Data Protection Act. In Japan, the Act on the Protection of Personal Information specifically deals with the transfer of citizens' personal data but only tangentially covers a data subject's right to privacy.

[6] Constitution of the Republic of Korea, Art 17.
[7] Constitution of the Republic of the Union of Myanmar, Art 357.
[8] Constitution of the Republic of Kazakhstan, Art 18.
[9] Constitution of the Socialist Republic of Vietnam, Art 11.
[10] Constitution of the Kingdom of Thailand B.E. 2560 (2017), Art 32.
[11] Constitution of the Democratic Socialist Republic of Sri Lanka of 1978, Art 14A.
[12] Constitutional Interpretation No 585 (15 December 2004) (Taiwan).
[13] Constitution of Cambodia, Arts 31 and 40.
[14] Constitution of the Republic of Singapore (2020 Rev. Ed. Sing.), Art 9(1).
[15] Constitution of the Republic of Indonesia 1945, Arts 28G(1), 28H(4) and 28J.
[16] W Prosser, 'Privacy' (1960) *California Law Review* 48, 3, 384.
[17] Personal Data Protection Law (Indonesia), Art 56.
[18] Personal Data Protection Act 2012 (Singapore), s 4(4)b.
[19] Personal Data Protection Ordinance (Hong Kong), s 33.

For practical purposes, many Asian states have sorted personal data into categories to facilitate regulation. Some jurisdictions divide personal data into two large categories, depending on the nature of the pieces of information involved. One category (involving data which are more closely related to an individual's privacy) will typically be subject to stricter regulations. For example, in Taiwan, the collection of 'specific personal data' is prohibited unless prescribed conditions are met. This category of 'specific personal data' includes medical records, medical treatment data, genetic information, sexuality, health examination, and criminal record.[20] These are considered more intimate types of personal information. On the other hand, the collection and processing of 'general personal data' will often be less stringently regulated. Thailand has a near identical classification of personal data to Taiwan in this regard.[21] Japan also has a similar system of binary classification, but instead of labelling categories as 'specific' and 'general', personal data is sorted into 'sensitive personal information' and 'non-sensitive personal information'. Kazakhstan accords heightened protection to an individual's health, religion, and biometric information. By contrast, the legislation in other states, notably Singapore, does not define 'sensitive personal data' or contain special categories of personal data to which more stringent regulations are applied.

The characterisation of data as 'personal' is not immutable but can be modified or even eliminated altogether by appropriate means. Through processes of anonymisation (converting personal data into a form which cannot be used to identify an individual), pseudonymisation (substituting parts of personal data with made-up values), and de-identification (removing certain parts of personal data through which an individual can be identified), information can cease to be 'personal' and become more readily transferrable and freely accessible. Asian jurisdictions typically allow for such processes to de-personalise data.

In many Asian jurisdictions, just as under GDPR, the right to privacy is not absolute. The right is subject to interference in certain circumstances as, for instance, when national security or criminal investigations are concerned. In evaluating whether an interference with the right to privacy is legitimate, Asian jurisdictions apply legal tests of varying standards of stringency. Some states, like Taiwan, allow a safe zone to public authorities for infringement of a citizen's right to privacy, to the extent that a government's conduct was aimed at fulfilling a statutory duty or obligation.[22] Another test that may be applied is that of proportionality. In other words, where a complaint of personal data infringement is made against a government agency, a court or other authority considering the case might ask itself:

1. whether the relevant agency had the power to conduct itself as it did;
2. whether the agency exercised any such power for a legitimate purpose;
3. whether the agency's conduct was no more than what was necessary to achieve the identified purpose; and
4. whether on balance the infringement of the individual's right to privacy was justified by the need to achieve the purpose.

[20] Personal Data Protection Act (Taiwan), Art 6.
[21] Personal Data Protection Act BE 2562 (Thailand), Ch A(c)(iv).
[22] Art 6, Personal Data Protection Act (Taiwan), Art 6.

As for remedies, Asian courts have readily granted relief (notably monetary compensation, injunctions and declarations) to prevent the continued breach of an individual's right to privacy.[23] But the bases of data privacy infringement claims vary from state to state. Some jurisdictions (such as Singapore) classify an action for breach of personal privacy as a statutory tort (for example, under Singapore's Personal Data Protection Act).[24] Complexity can arise when a controller or processor in state B infringes the privacy of a data subject in state A. In such situation, there is no one-size-fits-all solution among different Asian states. Some civil law countries (such as Indonesia and Thailand) apply the principle of *actor sequitur forum rei* with the result that a complaint should be lodged in the court of the place where the defendant is domiciled. Other states, such as Japan,[25] take multiple factors into account, including the defendant's domicile, the place of performance of a relevant obligation, the defendant's place of business, and the place of the wrong, before reaching a conclusion on a court's jurisdiction to hear an infringement complaint.

Nevertheless, a significant obstacle to effective data protection is the lack of a clearly applicable law in the situation where a data breach occurs in cyberspace and has potential ramifications in multiple states. To date, most jurisdictions have yet to enact local legislation to address the issue of applicable law in cases of multinational data breach. Therefore, the existing data protection legislation of many Asian states remain silent as to the issue of the law applicable and there may be overlapping assertions of jurisdiction.

IV. Summary of GDPR

Having identified GDPR as a backbone of data protection regulation in many Asian jurisdictions, this section summarises the principles underlying GDPR for readers who are not familiar with its terms.

GDPR comprises a Preamble and nine Chapters. The Preamble consists of 173 paragraphs and takes up nearly half of GDPR. In effect, the 173 paragraphs set out general principles of data privacy and protection which serve as a commentary on the interpretation and implementation of the rights and obligations contained in GDPR's nine chapters. This section will focus on the Preamble, summarising its key principles. It will then more briefly outline the contents of GDPR's nine chapters.

A. Preamble

From the outset, paragraph (1) signals that GDPR is about 'the protection of natural persons in relation to the processing of personal data'.[26] That is because 'everyone has the right to

[23] See, eg, Personal Data Protection Act 2012 (Singapore), s 48O.
[24] ibid, s 32.
[25] Code of Civil Procedure (Japan), Arts 3–9.
[26] Para (14) stresses that GDPR does not cover the processing of data belonging to legal persons, such as companies or business associations. But it appears that an individual may appoint an non-governmental organisation to act on his or her behalf when seeking a remedy for breach of the GDPR (see para (142)). On the special protection needed for the personal data of children, see para (38). On the special measures and care needed in handling

the protection of personal data concerning him or her'.[27] Such entitlement is 'a fundamental right' as affirmed by Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU). A consequence of this recognition is (as acknowledged in paragraph (2)) any principles relating to data privacy and protection must respect the rights and freedoms of natural persons regardless of nationality or residence. The aspiration is that the enactment of these principles will

> contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.

However, the right to have one's personal data protected is not absolute. This emerges from paragraph (4) which recognises that the right 'must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality'. There are trade-offs to consider when GDPR is being applied.

GDPR requires in paragraph (10) that, within the EU, there be a '[c]onsistent and homogenous application' of rules, not just to provide a high level of protection for data subjects, but also to remove 'obstacles to flows of personal data' among states. This paragraph thus picks up the theme of proportionality, suggesting that there is a balance to be struck between safeguarding a person's data on the one hand and ensuring access to information on the other. Nonetheless, within 'several sector-specific laws in areas that need more specific provisions', states are allowed a 'margin of manoeuvre' to enact their own laws as to the handling of 'sensitive data'. GDPR accordingly confers each state with some latitude (for example) on the extent to which an individual's privacy may be infringed in the interests of national security and the prevention of criminal activity.[28]

information which is 'particularly sensitive in relation to fundamental rights and freedoms', see paras (51) to (54). Examples are personal data on race or ethnic origin (para 51) or details relating to employment, social welfare, and health (especially where communicable diseases are concerned) (paras (52) to (54)). On employment and collective agreements, see also para (155).

[27] For examples of the width of what is comprised by the expression 'personal data', see paras 34 (genetic data) and 35 (health data).

[28] See further para (16) which expressly states that GDPR does not apply to 'activities concerning national security' and para (19) which excludes 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, including the safeguarding against and the prevention of threats to public security and the free movement of such data'. Note also para (20) dealing with data processing by courts and other judicial authorities. The gist of it is that GDPR applies to their activities, so that judges should be aware of their obligation under GDPR and should respond to complaints in their handling of personal data. Individual states may 'specify … operations and … procedures in relation to the processing of personal data by courts and other judicial authorities'. But any such laws 'should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary', enhance awareness among members of the judiciary of their obligations under this Regulation and handle complaints in relation to such data processing operations. Contrast the position in relation to '[p]ublic authorities to which personal data are disclosed in accordance with a legal obligation for the exercise of their official missions'. By para (31), such public authorities 'should not be regarded as recipients if they receive personal data which are necessary to carry out a particular inquiry in the general interest, in accordance with … law'. However, when requesting information, public authorities should always act in writing and provide reasons for their request. Their request 'should not concern the entirety of a filing system or lead to the interconnection of filing systems' and, in any event, processing of personal data by them 'should comply with the applicable data-protection rules according to the purposes of the processing'. In other words, although not treated as personal data recipients, public authorities are not entitled to be cavalier in the way that they handle information disclosed to them by individuals. They would still be under a duty to safeguard such information from wrongful disclosure or use.

Paragraph (13) introduces a different theme. It refers to the 'consistent monitoring of the processing of personal data' and 'equivalent sanctions in all Member States as well as effective cooperation between the supervisory authorities of different Member States'. This therefore provides that, to facilitate accountability in the handling of personal data, business enterprises should keep proper records of the data that they process.[29] Their records and record-keeping can then be monitored. Paragraph (15) adds that the record-keeping obligation must be technology neutral. The obligation arises regardless of whether an enterprise processes data by hand or automation.[30]

Paragraphs (22) to (25) have conflict of law implications. Paragraph (22) stipulates that GDPR should apply to any personal data processing by an establishment in the EU.[31] This is regardless of (1) whether such processing takes place in the EU or elsewhere and (2) whether the processing is done by a branch of the establishment or by a subsidiary with separate legal personality from the establishment. Paragraph (23) deals with the situation where the personal data of a data subject within the EU is processed outside the EU by a non-EU establishment.[32] In such case, GDPR will apply to processing activities 'related to offering goods or services to such data subjects irrespective of whether connected to a payment'. In determining whether the criterion for the application of GDPR has been met, one needs to consider the data processor's intentions, examining whether the establishment 'envisages offering services to data subjects in one or more Member States in the Union'. Paragraph (23) observes that the mere fact that an establishment's website may be accessed in the EU will not be enough to meet the criterion. Paragraph (24) adds that GDPR will also apply where the non-EU establishment is processing data for the purpose of 'monitoring ... the behaviour of [EU] data subjects in so far as their behaviour takes place within the [EU]'. The test is whether the relevant EU data subjects are being 'tracked on the internet', including through 'profiling ... particularly ... to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes'.[33]

[29] However, para (13) expressly exempts MSMEs (micro-, small and medium enterprises) having fewer than 250 employees from record-keeping obligations. Analogous exceptions from GDPR are found in para (18) (excluding 'the processing of personal data by a natural person in the course of a purely personal or household activity ... with no connection to a professional or commercial activity').

[30] For more on record-keeping, see the discussion on para (82) below.

[31] In determining a data controller's main establishment, reference might be made to para (36). In short, one needs to pinpoint the place of 'effective and real exercise of management activities determining the main decisions as to the purposes and means of processing'. This will not necessarily be the place where data processing is carried out. The presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute a main establishment and are therefore not determining criteria for a main establishment. Where relevant activities are carried out by several entities, the main establishment of the controlling entity should be regarded as the main establishment of the group, "except where the purposes and means of processing are determined by another undertaking".

[32] Para (80) stipulates that a non-EU establishment which processes the data of EU subjects must designate a representative (within the EU?) to serve as a point of contact with relevant EU public authorities. The representative In the case of breaches by the non-EU establishment, enforcement proceedings will be brought against the representative.

[33] On profiling, see also para (30): "Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, ... when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them." But this should be read as subject to para (70) (individual's right to object to being profiled, for the purpose of direct marketing). See further para (71) (discussed below).

Paragraph (25) concerns the application of GDPR to a non-EU establishment in a Member State's diplomatic mission or consulate.

Paragraphs (26), (28) and (29) deal with pseudonymisation and similar processes. GDPR will not apply where it is not possible to identify a person directly or indirectly from a data set because of pseudonymisation or similar processes.[34] This principle thus facilitates statistical research. Paragraph (27) adds that GDPR does not apply to the personal information of deceased persons.

Personal data may only be processed by a data controller or processor with the consent of the data subject or pursuant to some law (paragraph 40). Consent is defined in paragraph (32). It must be a 'freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her'.[35] This covers consent conveyed by electronic means. A data subject should not be made to indicate consent by silence, pre-ticked boxes or inactivity. If a request for information is made for several purposes, consent should be given for each purpose. Moreover, individuals should be entitled to limit their consent to what is compatible with the purposes of a given research project (paragraph (33)).

When data is to be processed by consent, the principle of transparency requires that 'any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used' (paragraph 41).[36] Details that should be drawn to a data subject's subjection include (1) the data controller's identity, (2) the purposes of the data processing, and (3) 'further information to ensure fair and transparent processing'. The latter category might comprise information on the risks, rules and safeguards involved and the data subject's rights. Any personal data obtained should be 'limited to what is necessary for the purposes for which they are processed'. Thus, the period for which personal data is to be stored must be no more than what is necessary for the relevant processes. There must be means to enable correction of inaccuracies or errors in the personal information obtained. Further, suitable measures must be taken for the security and confidentiality of the personal data disclosed. Under paragraph (42), a data controller should be able to show that an individual has consented to the processing of his or her data. Standard form consents drafted by a controller should be 'in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms'. Individuals should know who the data controller is and the purposes for which the personal data supplied are to be used are intended. Paragraph 42 warns: 'Consent should not be regarded as freely given if the data subject ... is unable to refuse or withdraw consent without detriment'.

In contrast, where data is to be processed by a government authority in the public interest, it must be under a law authorising the operation and identifying its purpose (paragraph (45)). Further, the law

> could specify ... general conditions ... governing the ... data processing, [such as] specifications for determining the controller, the type of personal data ... subject to the processing, the data

[34] See also para (57) on obtaining further information to enable an anonymised data subject to be identified.

[35] However, in consequence of para (43), consent will not be treated as freely given (and cannot be taken as the basis for processing of personal data) where there is 'a clear imbalance between the data subject and the controller, in particular where the controller is a public authority'.

[36] On transparency, see further para (58).

> subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage period and other measures.

In this regard, processing will be lawful and necessary when done to protect the life of the data subject or another natural person (paragraph (46)).

Paragraphs (46) to (50) provide instances of data processing that may be regarded as legitimate. This involves a balancing of the legitimate interests of a data controller with those of a data subject. For instance, a controller will have a legitimate interest to process data to obviate fraud (paragraph (47)). Interestingly, paragraph (47) suggests that processing for direct marketing purposes 'may' be a legitimate interest. Under paragraph (48), data controllers belonging to a group 'may' have a legitimate interest in sharing data with other members of the group for administrative reasons. By paragraph (49), data processing in the interests of network and information security also constitute a legitimate interest, if done proportionately. As for processing beyond the purposes for which consent has been given or beyond the authority conferred by law, that will only be possible 'where the processing is compatible with the purposes for which the personal data were initially collected' (paragraph (50)). Examples would be the archiving of data, the conducting of research, or the compilation of statistics. Another instance would be the disclosure of information to the police or other competent authority in criminal cases. But such transmission can be constrained by 'legal, professional or other binding obligation of secrecy'.

A corollary to transparency in data collection is the need for the implementation of a system whereby a data subject can readily obtain, correct or delete information about him or her. The requisites of such a system are covered by paragraphs (59) to (69). For instance, information need not be provided

> where the data subject already possesses the information, where the recording or disclosure of the personal data is expressly laid down by law, or where the provision of information to the data subject proves to be impossible or would involve a disproportionate effort (paragraph (62)).

Importantly, a data subject has the 'right to be forgotten' (that is, the right to have personal information deleted) when data is 'no longer necessary in relation to the purposes for which they [were] collected or otherwise processed', when consent for collection is withdrawn, or where there has been non-compliance with law (paragraph (65)).

Given rapid developments in the use of artificial intelligence (AI) in data processing, paragraph (71) should be noted. It confirms an individual's right 'not to be subject to a decision … evaluating personal aspects relating to him or her … based solely on automated processing and which produces legal effects concerning him or her'. Examples are the denial of an online credit or employment application without human involvement. But a balancing exercise is involved. If, for instance, a question of fraud or tax-evasion is involved, profiling may be permissible, subject to adequate protections.

Paragraph (82) returns to the theme of record-keeping. Data controllers and processors must keep records of their processing and cooperate with government authorities supervising their activities, including providing access to their records. Data controllers and processors need to consider the risks involved in their processing activities and take appropriate security measures (including encryption) to safeguard such processes and any information collected (paragraph (83). Measures include 'taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected'. Where the risks are high and the consequences of breaches of an individual's privacy are great, a 'data protection impact assessment' (DPIA) ought to be undertaken (paragraph (84)). If a DPIA concludes that the establishment's data processing entails 'a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation',[37] reference should be made to the relevant supervisory authority on ways of mitigating the effects of data breaches.[38] In the event of a significant data breach, paragraph (85) states that 'the controller should notify … the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it'. In addition, a data subject whose data has been compromised, should be informed of the breach as soon as possible, together with 'recommendations … to mitigate potential adverse effects' (paragraph (86)).

Paragraph (101) affirms the importance of '[f]lows of personal data to and from countries outside the [EU] and international organisations … [to] the expansion of international trade and international cooperation'. But flows should not compromise the data protection standards in GDPR, especially when personal data is passed to a non-EU state and from there to another state. Thus, without prejudice to treaties or conventions (see paragraph (102)), 'transfers to third countries and international organisations may only be carried out in full compliance with [GDPR]'. For this purpose, the European Commission is empowered to determine for all EU members whether a non-EU state has implemented 'an adequate level of data protection'. This is intended to provide certainty and uniformity within the EU as regards non-EU countries.

Paragraph (104) sets out the factors that the European Commission should take into account when making a determination. Factors include: (1) the 'fundamental values on which the [EU] is founded'; (2) respect for the rule of law in the non-EU state; (3) 'access to justice as well as international human rights norms and standards'; and (4) the non-EU state's 'general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law'. Paragraph 104 adds that the non-EU state should: (1) 'offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the [EU]'; (2) 'ensure effective independent data protection supervision'; (3) 'provide for cooperation mechanisms with the Member States' data protection authorities'; and (4) provide data subjects with 'effective and enforceable rights and effective administrative and judicial redress'. The Commission is supposed to review its determinations regularly (paragraph (106)) and can decide that a non-EU state no longer meets the GDPR standard (paragraph (107).

Where a non-EU state does not meet GDPR standards, data controllers and data processors should 'compensate for the lack of data protection … by way of appropriate safeguards for the data subject' (paragraph (108)). Measures would include 'binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority, or contractual clauses authorised by a supervisory authority'. In limited situations (such as legal necessity[39]), it should also be possible for data to be transferred to non-EU states where a data subject expressly consents (paragraph (111)). On the extraterritorial effect of legislation in non-EU states purporting

[37] Eg, this may be the situation where there is large scale data processing done on a regional, national or international level (see para (91)).

[38] On consultation with the supervisory authority generally, see further paras (92) to (96).

[39] For examples of legal necessity, see paras (112) and (113).

to affect data subjects within the EU, paragraph (115) provides that transfers of personal information should only be allowed where the requirements of GDPR are met. In this vein, paragraph (116) proposes the establishment of cross-border cooperation with data supervisory authorities outside the EU on a reciprocal basis.[40]

Paragraphs (119) to (123) deal with the independence, funding, resources, responsibilities and duties of supervisory authorities. However, paragraph (118) observes that supervisory authorities, no matter how independent, should be subject to judicial review. As an additional safeguard, a European Data Protection Board (EDPB) is to be set up to ensure GDPR's consistent application in the EU. Details of the EDPB are set out in paragraphs (140) and (141).

Paragraph (143) concerns applications by natural or legal persons to annul the EDPB's decisions on remedies (including damages[41] and penalties[42]) against actions by supervisory authorities. Paragraph (145) deals with proceedings against data controllers or processors. Except where the complaint is against a supervising authority, claimants may choose between commencing proceedings in the state where a controller or processor has an establishment or in the place where the data subject resides. General rules on jurisdiction within the EU are subject to the latter special jurisdictional rule (paragraph (147)). There may also be fines and criminal sanctions for infringements of GDPR (paragraph (148)).

Paragraph (153) highlights the need to balance the right to privacy against the right to freedom of expression. It states: 'Member States law should reconcile the rules governing freedom of expression and information, including journalistic, academic, artistic and or literary expression with the right to the protection of personal data pursuant to this Regulation'. It is left to Member States to decide how the balance between the competing rights is to be drawn. Where the resulting domestic laws are different, then 'the law of the Member State to which the controller is subject should apply'.

Paragraph (154) concerns personal information in official documents to which members of the public are granted access in the public interest. Paragraph (156) to (163) impose safeguards on data processing for archiving, historical, scientific and statistical purposes. Paragraph (165) preserves the constitutional rights of churches and religious associations.

Paragraphs (166) to (170) confer power on the Commission and the EU to implement specified measures in connection with data protection and privacy.

B. Chapters

The main body of GDPR is divided into 11 chapters, entitled: (I) General Provisions; (II) Principles; (III) Rights of Data Subject; (IV) Controller and Processor; (V) Transfers of Personal Data to Third Countries or International Organisations; (VI) Independent Supervisory Authorities; (VII) Cooperation and Consistency; (VIII) Remedies, Liability and Penalties; (IX) Provisions Relating to Specific Processing Situations; (X) Delegated Acts and Implementing Acts; and (XI) Final Provisions.

[40] See also paras (124) to (138) on mechanisms of cooperation among supervisory authorities, where data protection in more than one state is involved, including on instituting a 'one-stop-shop mechanism' (especially paras (127) and (128)) and ensuring consistency (paras (135) and (136)). On a one-stop-shop, see further para (141): 'Every data subject should have the right to lodge a complaint with a single supervisory authority ... in the Member State of his or her habitual residence, and the right to an effective judicial remedy ... if the data subject considers that his or her rights under this Regulation are infringed'.

[41] See para (146).

[42] See para (148).

i. Chapter I (General Provisions)

Article 1 sets out the two principal norms which GDPR seeks to balance: (1) 'the rights and freedoms of natural persons and in particular their right to the protection of personal data' and (2) 'the free movement of personal data'. Article II affirms that GDPR is technology neutral and sets out what is excluded from the purview of GDPR. In that respect, data processing by a natural person as part of 'a purely personal or household activity' falls outside the scope of GDPR. Article 3, on the other hand, provides for GDPR's extraterritorial effect. GDPR will apply to data processing by a controller or processor within the EU, regardless of where the processing takes place. Conversely, it also applies to the processing of data belonging to data subjects in the EU, regardless of where a controller or processor is situated. For the purposes of Article 3, 'processing' involves

> (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

Article 4 defines terms (such as 'personal data', 'processing', 'controller', 'consent', and 'supervisory authority') used throughout GDPR.

ii. Chapter II (Principles)

The chapter sets out the key principles underlying data processing. Of primary interest is Article 5(1) which constrains the extent to which personal data may be processed, used and stored, to no more than what is necessary for a legally valid purpose:

Personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall ... not be considered to be incompatible with the initial purposes ('purpose limitation');
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes

or statistical purposes … subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Article 6 specifies when data processing is lawful. Essentially, processing is lawful if it is done with the consent of a data subject, pursuant to a legal obligation or duty, or as a matter of necessity in the public interest. Article 7 enumerates the conditions for a valid and binding consent by a data subject. Article 8 deals with consent by children, while Articles 9 and 10 deal with the processing of special categories of data (information about an individual's race, ethnic origin, political views, religion, health, sex life, orientation, and criminal record). Article 11 is about processing in cases where it is not necessary to identify individuals.

iii. Chapter III (Rights of Data Subject)

Chapter III is divided into five sections. The first four sections deal with specific rights of a data subject. Section 1 focuses on the right to transparency. Section 2 details a subject's right to be informed about processing operations relating to him or her (whether the personal data being processed has been obtained from the subject or not) and to have access to the personal data collected. Section 3 deals with a subject's right to rectification of personal data, the right to have the same erased (that is, the right to be forgotten), and the right to restrict the processing of personal data. Article 20 refers to portability, that is, the right to receive personal data in a 'structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance'. Section 4 confers a right to object to decisions being taken by automated processing, including by profiling.[43]

Section 5 implicitly acknowledges that the rights in the previous four sections are not absolute. Article 23(1) authorises the EU or Member States to limit such rights by legislation. But this is only provided 'the essence of the fundamental rights and freedoms' is respected, and the restriction is 'a necessary and proportionate measure in a democratic society' for safeguarding:

a) national security;
b) defence;
c) public security;
d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;

[43] GDPR, Art 4 defines 'profiling' as 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements'.

f) the protection of judicial independence and judicial proceedings;
g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);
i) the protection of the data subject or the rights and freedoms of others; and
j) the enforcement of civil law claims.

Additionally, Article 23(2) stipulates that any restrictions must identify:

a) the purposes of the processing or categories of processing;
b) the categories of personal data;
c) the scope of the restrictions introduced;
d) the safeguards to prevent abuse or unlawful access or transfer;
e) the specification of the controller or categories of controllers;
f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;
g) the risks to the rights and freedoms of data subjects; and
h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

iv. Chapter IV (Controller and Processor)

Chapter IV deals with the duties and responsibilities of data controllers and processors. It is in five sections. Section 1 is on general obligations of controllers and processors. Article 30 imposes a duty to keep proper records, while Article 31 requires them to cooperate with supervisory authorities. Section 2 imposes duties on controllers and processors to maintain the security of personal data, 'taking into account the state of art'. Such duties include the duty to inform supervisory authorities and data subjects of significant breaches of personal data.[44] Section 3 concerns the need to carry out DPIAs. Section 4 requires controllers and processors to appoint data protection officers. Section 5 encourages Member States, supervisory authorities, the European Commission, the EDPB, and others (1) to draw up codes of conduct on the application of GDPR, and (2) to set up institutions and means for data protection certification as a way of establishing compliance with GDPR.

v. Chapter V (Transfers of Data to Personal Data to Third Countries or International Organisations)

Chapter V enacts rules for assessing whether data may be transferred to non-EU states or international bodies. The general principle is in Article 44:

> Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if … the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation

[44] See Arts 33 and 34.