Assessment of the Republic of Korea

Personal Information Protection Act 2011 ("PIPA")

for an Adequacy Recognition Decision

by the

Dubai International Financial Centre Authority

("DIFC" or "DIFCA")

Office of the Commissioner of Data Protection

DIFC

Table of Contents

DIFC

Introduction

Articles 26 and 27 of the Data Protection Law, DIFC Law No. 5 of 2020 and Section 5 of the DIFC Data Protection Regulations 2020 (the "DIFC DP Law 2020"[1]) address transfers of Personal Data to Third Countries or International Organisations. Article 26(2) specifically states:

> *For the purposes of Article 26(1), the Commissioner may determine from time to time that a Third Country, a territory or one (1) or more specified sectors within a Third Country, or an International Organisation ensures an adequate level of data protection*.

Such adequacy recognition is based on an assessment of key data protection concepts and obligations found in a jurisdiction's data protection laws to ensure equivalence with the local data protection law. As such, the DIFC Office of the Commissioner of Data Protection (the "DIFC Commissioner") assesses the Republic of Korea's laws and regulations according to the following criteria:

1. Basic data protection concepts and definitions
2. Grounds for lawful and fair processing for legitimate purposes
3. Existence of Data Protection Principles
    a. purpose limitation
    b. data quality and proportionality
    c. data retention
    d. security and confidentiality
    e. transparency
4. Data Subjects' Rights
5. International / Onward Data Transfer Restrictions
6. Security of Processing and Breach Reporting
7. Accountability and Enforcement
8. Additional content principles for specific types of processing, such as:
    a. Special categories of data (aka sensitive personal data)
    b. Direct marketing
    c. Automated decision making and profiling
9. Existence of international commitments and conventions binding on the Republic of Korea or its membership of any multilateral or regional organisations.

[1] *All definitions and capitalized terms herein, including the definition of the DIFC Data Protection Commissioner, are as set out in DIFC DP Law 2020, Schedule 1, Art. 3.*

Summary of the Republic of Korea's Applicable Laws and Regulations

The Constitution of the Republic of Korea recognises the Right to Privacy as a fundamental right that is to be protected and preserved, and provides a basis for protection of privacy and data protection for both citizens and foreign nationals.[2] Korea is a Party to several international agreements that guarantee the right to privacy, such as the International Covenant on Civil and Political Rights (Article17), the Convention on the Rights of Persons with Disabilities (Article 22) and the Convention on the Rights of the Child (Article 16)[3].

The current Korean data protection regime is composed of the Personal Information Protection Act ("PIPA", as last amended by Act No. 16930 of 4 February 2020) which is the general and comprehensive statute for data protection enacted in March 2011 and amended in February 2020, including certain provisions of the Act on Promotion of Information and Communications Network Utilization and Information Protection, 2016 (Network Act); and other special sector specific laws including the Use and Protection of Credit Information Act 2009 ("UPCIA") (as amended) regulating personal credit information.

Where a provision of a special sectorial law is found to be applicable to an entity, the entity must comply with the provision of the sectoral law ahead of PIPA. Nevertheless, their basic data protection principles are also similar.

Therefore, the Personal Information Act ("PIPA") is of the main point of review for the purposes of this adequacy decision. PIPA is supplemented by an Enforcement Presidential Decree ('PIPA Enforcement Decree')[4], equally legally binding and enforceable. Because the DIFC does not permit retail banking or lending as a business activity, this assessment does not the processing of personal credit information pursuant to the UPCIA by controllers that are subject to oversight by the Financial Services Commission.

The Commissioner's Office has reviewed the PIPA together with relevant supplemental provisions, as well as supporting documentation from other authorities, and provides its findings below.

[2] *Constitution of the Republic of Korea, 1948 [Article 17-18]:* https://www.refworld.org/docid/3ae6b4dd14.html

[3] *Please see EU Adequacy Decision, p3 footnote 16:* https://ec.europa.eu/info/sites/default/files/1_1_180366_dec_ade_kor_new_en.pdf

[4] *Enforcement Decree of the Personal Information Act:* https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=54521&type=part&key=4

Observation 1: Basic data protection concepts and definitions

Concepts:

PIPA is aimed at *"protecting the freedom and rights of individuals, and further, to realize the dignity and value of the individuals, by prescribing the processing and protection of personal information."* These objectives are similar to the DIFC DP Law provided for in Part 1 - Article 5 as well as the basis of Council of Europe Convention 108.

PIPA is applicable to a controller or processor that is an individual; a public agency; a juridical person; or an organisation that by itself or through a third party, processes personal information in relation to its business or organisational activities.

This includes personal information processed electronically and manually. The DIFC DP Law 2020 covers both automated and manual processing when the data forms or is to form part of a filing system, as set out in Part 1 – Article 6(2).

Registration and notification of personal data processing activities only applies to public agencies and not private sector companies.

The DIFC DP Law 2020 provides for a registration requirement in Article 14 (7), however, it applies to private sector companies.

Article 3 (1) - (8) of PIPA provide that a personal information controller must explicitly specify the purposes of his/her processing operations, and collect the personal information to the minimum extent necessary for such purposes in a fair and legitimate manner. Controllers must also ensure that the personal information processed is accurate, kept up to date, and complete in line with the processing purposes.

Controllers are also required to implement secured processing methods that take into account the assessment of potential risks that may lead to infringement on data subjects' rights, and endeavor to gain the trust of data subjects by performing such duties and responsibilities. Anonymization or pseudonymisation may be employed a further security measure.

Article 3 of PIPA on the Principles for Protecting Personal Information is essentially equivalent to the General requirements contained in Article 9 of the DIFC DP Law of 2020.

There are certain limits on applicability of PIPA's provisions regarding the collection and use of personal information (Article 15), the methods for obtaining consent (Article 22), notification on transfer of personal information following business transfer, etc. (Article 27(1)-(2)), data breach notification (Article 34), and the suspension of processing of personal information (Article 37), do not apply to the processing of personal information made via visual devices located in public places.

Please note, in addition to the above, the provisions on accountability contained in Articles 15, 30, and 31 do not apply to any personal information processed to operate a group or association for friendship, such as an alumni association or hobby group.

Article 58 of PIPA provides that data protection requirements in Chapter III to VII[5] under PIPA exclude from its scope the following categories of personal information:

- Collected or requested for processing by public institution under the Statistics Act. The EU Adequacy Decision notes that "…personal data processed in this context normally concerns Korean nationals and might only exceptionally include information on foreigners, namely in the case of statistics on entry to and departure from the territory, or on foreign investments. However, even in these situations, such data is normally not transferred from controllers/processors in the Union, but would rather be directly collected by public authorities in Korea."[6]

- Collected or requested for the analysis of information related to national security, which is limited, and subject to rules on oversight, enforcement and redress, and more specific obligations to only process personal data only to the extent and for as long as is needed to achieve the purpose. Safety measures must in any case be applied, there are several limitations outlined in relevant applicable laws including the need for warrants, lawful interception restrictions and a complaints process must be available for lodging grievances;

- Processed, collected or used for reporting by the press, missionary activities, and nomination of candidates by political parties, or temporarily where urgently necessary for public safety, health, security, etc.

Article 59 of PIPA also provides for a list of Prohibited Activities, setting out that entities processing personal information must not undertake any of the following activities:

- Acquiring personal information or obtain consent to personal information processing by fraud, improper or unjust means;

- Divulging personal information acquired in the course of business, or providing it to a third party without authority to do so;

- Damaging, destroying, altering, forging, or divulging other's personal information without legal authority or beyond proper authority.

Sensitive Information is defined in Article 23 of PIPA and the scope is further clarified in Article 18 of the PIPA Enforcement Decree. It includes personal data revealing information about the ideology, belief, admission to

[5] *Chapter: III. Processing of Personal Information, IV. Safeguard of Personal Information, V. Guarantee of Rights of Data Subjects, VI. Special Cases Concerning Processing of Personal Information by Providers of Information and Communications Services or Similar, VII. Personal Information Dispute Mediation Committee*.

[6] *EU Adequacy Decision, p8*

or withdrawal from a trade union or political party, political opinions, health, and sexual life of an individual, as well as other personal information that is likely to threaten the data subject's privacy "noticeably". Article 18 of the updated PIPA Enforcement Decree adds that biometric information, DNA acquired from genetic testing, and data that constitutes a criminal history record are also considered sensitive information.

These categories as well as the requirements for such processing are to a large extent similar to the considered Special Categories personal data under Article 11 the DIFC DP Law 2020.

Definitions:

Definitions are found in Chapter 1, Article 2 of the PIPA. Most of the defined terms therein are substantially similar to the provided in the DIFC DP Law 2020, Schedule 1, Article 3, when interpreted accordingly, including the terms: personal information (data), data subject, processing, personal information file, controller, and public institutions as similarly defined in Article 28 DIFC DP Law 2020.

PIPA also defines the terms "scientific research" and "visual data processing devices" with respect to scope in protecting the freedom and rights of individuals. Pseudonymous information, which is de-identified data that cannot be used to identify a specific individual without additional information to restore it to its original state, is considered personal data under PIPA.

The main Personal Data principles under PIPA are substantially the same as in the DIFC, as follows:

- Consent Obligation
- Purpose Limitation
- Privacy Notices
- Access and Correction
- Accuracy
- Protection / Security
- Retention Limitation
- Transfer Limitation
- Data Breach Notification
- Accountability

Article 7 PIPA provides for the Personal Information Protection Commission ("Protection Commission" or "PIPC") to act as an independent authority whose work is to protect personal information and its processing. The Commission is established under the Prime Minister. Although the presence of an independent regulatory authority does not guarantee certainty regarding protection of personal data, it shows a degree of commitment toward the protection of personal information and preservation of individual privacy.

Observation 2: Grounds for lawful and fair processing for legitimate purposes

Article 15 to 19 of PIPA set out the legal basis for processing personal information.

According to Article 15, a controller may only access, collect, use, share, or disclose personal information in the following scenarios:

- Where they have received consent from a data subject;
- if special provisions exist in other laws or it is inevitable to observe legal obligations, if it is inevitable for a public institution's performance of its duties under its jurisdiction as prescribed by statutes, or any relevant measures and policy;
- if it is inevitably necessary to execute and perform a contract with a data subject;
- if it is deemed manifestly necessary for the protection of life, bodily or property interests of the data subject or third party from imminent danger where the data subject or their legal representative is not in a position to express intention, or prior consent cannot be obtained owing to unknown addresses, etc.;
- if it is necessary to attain the justifiable interest of a personal information controller, where such interest is manifestly superior to the rights of the data subject.

Moreover, processing must be minimized and is allowed to the extent that it is substantially related to the justifiable interest of the controller and does not go beyond a reasonable scope[7], which is substantially similar to the requirements and obligations found in Articles 10 and 11 of the DIFC DP Law 2020.

Personal information controllers are required to inform data subjects of the following when obtaining consent:

- The purpose of the collection and use of personal information;
- Particulars of personal information to be collected;
- The retention period of personal information;
- The fact that the data subject is entitled to withdraw consent, as well as disadvantages, if any, resulting from such withdrawal.

Personal information may be processed without the consent of a data subject in so far as the disadvantages that could be caused to the data subject are weighted and necessary measures have been taken to secure the personal information such as the use of encryption, etc. This is a new provision from the 2020 amendments, and is aligned with the requirements of the DIFC DP Law 2020. [8]

[7] *PIPA Article 15*

[8] *PIPA Article 17*

Article 16 PIPA asserts that Controllers may only collect the minimum required information necessary to attain the specific purpose. The burden of proof that the necessary has been achieved shall be borne by the personal information controller.

These requirements are in alignment with the provided in Articles 9, 10, 11 and 12 of DIFC DP Law 2020 regarding consent as a basis for lawful processing.

Observation 3: Existence of Data Protection Principles

Data protection principles under the PIPA are set out below.

1. Consent

A personal information controller may only collect, and process the personal information of data subjects who have consented to collection and processing. Data subjects have the ability/right to withdraw consent upon reasonable notice of such withdrawal. Where a data subject provides a notice to withdraw consent, the controller must cease the collection and processing of their personal information.

This obligation is similar to those set out in Articles 12, 22 and 32 of the DIFC DP Law 2020.

2. Purpose Limitation

A personal information controller may only collect and process the personal information of data subjects for the purpose for which consent has been given. Consent can never be mandatory for any purpose given by the Organisation to provide a particular product or service unless consent is required for a reasonable purpose of providing such service.

Article 18(4) states:

> *Where a public institution uses personal information, or provides it to a third party for other purpose than the intended one pursuant to the subparagraphs of Article 18(2) PIPA, it shall post the legal grounds for such use, purpose, and scope, and all related matters on the Official Gazette or on its website requirements for such use or provision including the legal basis, purpose, scope, etc.. The publication shall contain the name of the personal information or such file, the name of the institution using the personal information as well as its purpose, the statutory ground for such use or access, the items of personal information to be used or provided, the date, frequency or period to use or provide personal information, the manner of use or being provided, or any restriction from the recipient pursuant to Article 18(5) of PIPA.*

These obligations are similar to Article 9(1)(c) of the DP Law 2020 on purpose limitation.

3. Privacy notices

Under PIPA, a personal information controller shall notify data subjects in advance of the purpose for which their Personal information is being collected, processed, or disclosed, as well as the method for withdrawing consent.

When a personal information controller processes a data subject's personal information collected from a third party, they shall immediately notify the data subject at their request of the source of collected personal information; the purpose of processing personal

information; the fact that the data subject is entitled to demand suspension of processing of personal information.

Privacy notices are a requirement under Articles 29 and 30 of the DIFC DP Law 2020, and the requirements in PIPA are sufficiently similar.

4. Access and Correction

Upon receipt of a request for access filed by a data subject, a personal information controller is obliged to provide information to individuals, upon request and as soon as reasonably possible, regarding:

- what Personal Data of theirs is in the controller's possession or under their control (both private and public entities) as well as the purpose of collection and use of such data;

- within a period of 10 days from the day of receipt of the access receipt.

A data subject who has accessed their personal information may request correction of their personal information from the controller provided that this is not prohibited by other statutes. The controller shall immediately take the necessary measures to exercise the correction, including investigation of the request, and inform the data subject of the rectified result.

Such access may be limited or denied where prohibited or limited by statutes, where it may cause damage to the life or body of a third party, where a public institution will be prevented from performing its duties such as the imposition, collection or refund of taxes, for evaluation of academic achievements or admission, testing, and qualification, as well as ongoing evaluation or decision-making in relation to a grant assessment.

These requirements are substantially similar to those found in Articles 9(1)(f) and Articles 32 to 40 of the DP Law 2020 on the application of Data Subjects rights.

5. Accuracy and Minimisation

A personal information controller must ensure that the Personal information it collects is accurate, complete, and up to date to the extent necessary for the purpose of his/her processing, and that any data collected should be the minimum required to achieve the intended purposes**.**

This provision is similar to Article 9(1) (g) of the DP Law 2020.

6. Protection / Security (Article 29 of the Personal Information Safeguard and Security Standard)

Personal information controllers shall take all technical, managerial, and physical measures to establish an internal management system necessary to ensure safety and prevent the lost, theft, alteration, forgery or damage to personal information. [9]

This requirement is found in Article 9(1)(i) of the DP Law 2020.

7. Retention

Where retention is not mandatory under other statutes, a personal information controller is required to destroy personal information when it becomes unnecessary, owing to the expiry of the retention period, attainment of the purpose of processing the personal information, etc.

This requirement is found in Article 9(1)(h) of the DP Law 2020.

8. Cross Border Transfers

Under PIPA, the protection of information transferred overseas is specifically provided in regard to information and communications service providers. If a data subject's information is transferred overseas, Online Service Providers must obtain the subject's consent in respect to the specific information to be transferred, the destination country, the date, time, and method of transmission, the name of the recipient and the contact information of such person in charge, as well as the recipient's purpose of the use of the personal information and its retention period.

As per the safety requirement contained in Article 29 of the PIPA, a similar requirement is found in Article 27 of the DP Law 2020.

In South Korea, binding corporate rules are not seen as a sufficient basis for cross border transfers. Therefore, where approved elsewhere, the exporting organisation must utilise another method of legitimising the transfer or onward transfer.

9. Data Breach Notifications

When a personal information controller becomes aware of a data breach, they shall immediately inform data subjects of the details of the data constituting the breach; when and how has the breach occurred; as well as ways in which the subjects can minimize the risk of damage and report damage.

[9] See the Personal Information Safeguard and Security Standard
http://privacy.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_000000000830758&fileSn=0&nttId=8186&toolVer=&toolCntKey_1=

Where a breach affecting 1,000 or more subjects takes place, the controller shall immediately notify the subjects, and the Data Protection Commissioner, or any designated specialized institution.

Similar requirements are found in Articles 41 and 42 of the DP Law 2020.

10. Accountability

A personal information controller should be transparent and accountable for its data protection practices, policies and complaints processes upon request. This includes maintaining privacy policies, appointing someone responsible for data protection operations, such as a privacy officer or chief privacy officer and must also provide a way of contacting the DPO.

Similar requirements are found in Articles 14 to 22 of the DP Law 2020.

11. Transparency

All data subjects should be informed of the main features of the processing of their personal data and controller's privacy policies must be made public e in such a way that data subjects "may recognise it with ease" (Article 30(2)). PIPA requires controllers to notify data subjects of conditions where processing exceeds certain thresholds, including the source of the information, the purpose of processing and the data subject's right to demand a suspension of processing, unless such notification proves impossible due to the lack of any contact information.

Limited exceptions apply for certain personal information held by public authorities, in particular files that contain data processed for national security, other particularly important or sensible national interests, or criminal law enforcement purposes, or where notification is likely to cause harm to the life or body of another person, or unfairly damages the property and other interests of another person, however only where the public or private interests at stake are superior to the rights of the data subjects concerned (Article 20(4) PIPA). This requires a balancing of interests.

Observation 4: Data Subjects Rights (DSR)

Chapter 1 – Article 4, PIPA affords certain legitimate rights to data subjects to be enforced on controllers. To this end, PIPA also has prescriptive procedural rules to ensure data subjects' exercise of such rights.

These rights include:

- the right to be informed of the processing of their personal information;
- the right to determine whether or not to consent and the scope of consent regarding the processing of such personal information;
- the right to confirm whether or not personal information is being processed and to request access (including the provision of copies; hereinafter the same applies) to such personal information;
- the right to suspend the processing of, and to request correction, deletion, and destruction of such personal information; and
- the right to appropriate redress for any damage arising out of the processing of such personal information through a prompt ad fair.

Such rights may be subject to certain restrictions, insofar as these restrictions are necessary and proportionate to safeguard important objectives of general public interest.

Chapter 5, Articles 35 to 39 provide substantial detail regarding these rights as well as remedies, which are effectively reflected in the DIFC DP Law 2020 Articles 32 to 40 and Part 9[10]. A data subject who has reviewed his personal information held by the personal information manager may request that his or her personal information be corrected or deleted. However, there are certain instances which limit such rights, such as when retention of personal information is required by law.

Where a data subject intends to request access to his or her own personal information from a public institution, the data subject may request such access directly from public institution or indirectly via the Protection Commissioner as provided by presidential decree. They have the right to object to direct marketing, and to revoke consent at any time.

In instances where a controller has collected personal information from a third party (i.e. transferred data), data subjects generally have the right to receive information about the source of the personal data collected (i.e. the transferor), the purpose of processing and the fact that the data subject is entitled to demand suspension of processing as per Article 20(1) of PIPA.

There are limited exceptions to such notifications in cases where the latter is likely to endanger the life or body of another person or to unfairly damage the property and other interests of another person where such interest are superior to the data subject's rights. (Article 20(4) PIPA). Risk of the above must be accordingly assessed.

[10] *Please see DIFC Rights and Remedies table at this link:*
https://www.difc.ae/application/files/5116/3634/9864/Data_Subject_Rights_and_Remedies.pdf

Suspension of processing is addressed specifically in Article 37. The right to suspension of processing also applies where personal data is used for direct marketing purposes, such as in order to promote or solicit the purchase of goods or services. Failure to suspend this type of processing may lead to criminal sanctions (Article 73(3) PIPA).

Additionally, when requesting consent for direct marketing, the controller must inform the data subject in particular of the intended use of the data for direct marketing purposes.

To facilitate the exercise of individual rights, the controller must establish dedicated procedures and announce them publicly as per Article 38 PIPA. Such includes procedures for raising objections against the denial of a request. The controller must ensure that the procedure for exercising DSR is clear, simple, and easy to understand.

Article 28(7) PIPA provided further data subjects' rights on pseudonymous data.

Observation 5: International Data Transfers

Article 14 of PIPA requires the government to "establish policy measures necessary to enhance the personal information protection standard in the international environment", in order to protect data subject's rights where data is transferred across borders.

In this respect, regarding special cases concerning processing of personal information by providers of information and communications services, PIPA distinguishes between (1) the outsourcing of processing to an outsourcee (i.e. a processor) and (2) the provision of personal data to third parties located abroad.

(1). Outsourcing of processing to an outsourcee: When the processing of personal data is outsourced to an entity located in a third country, the Korean controller has to ensure compliance with PIPA's provisions on outsourcing (Article 26 PIPA)[11].

This includes putting in place a legally binding instrument that among others limits the processing by the outsourcee to the purpose of the outsourced work, imposes technical and managerial safeguards and limits sub-processing; and publishing information on the outsourced work.

In addition, the controller is under an obligation to "educate" the outsourcee on necessary security measures and supervise, including through inspections, compliance with all the controller's obligations under PIPA as well as the outsourcing contract.

If the outsourcee causes damage by processing the personal data in violation of PIPA, the controller will be remain liable.

Information and communication service providers must obtain consent of the user for any transfer of personal information overseas. In case personal information is transferred as part of the outsourcing of processing operations, including for storage, consent is not required if the individuals concerned have been informed, directly or through public notice in a way that allows easy access, in advance of the particulars of the information to be transferred, the country to which the information will be transferred as well as the date and method of the transfer, the name of the recipient and the purpose of use and retention by the recipient. In addition, the general requirements for outsourcing will apply in that case.

For each transfer, specific safeguards must be put in place with respect to security, the handling of complaints and disputes, as well as other measures necessary to protect users' information (Article 48-10 PIPA Enforcement Decree).

The controller remains responsible for the personal data that has been outsourced and must ensure that the overseas processor processes the information in accordance with PIPA.

[11] *PIPA Article 26(7): Article 15 through 25, 27 through 31, 33 through 38, and 59 shall apply mutatis mutandis to outsourcees.*

If the outsourcee processes the information in violation of PIPA, the Korean controller can be held responsible for a failure to comply with its obligation to ensure compliance with PIPA, such as through its supervision of the outsourcee.

The safeguards included in the outsourcing contract and the responsibility of the Korean controller for the actions of the outsourcee ensure continuity of protection when personal data processing is outsourced to an entity outside of Korea.

(2). Provision of personal data to third parties located abroad: Controllers may provide personal data to a third party located outside of Korea. While PIPA includes a number of legal grounds allowing for the provision to third parties in general, if the third party is located outside of Korea, the controller in principle has to obtain the data subject's consent after having provided the data subject with information on the type of personal data, the recipient of the personal data, the purpose of transfer in the sense of the purpose of processing pursued by the recipient, the retention period for processing by the recipient as well as the fact that the data subject may refuse to consent (Article 17(2), (3) PIPA).

Transparency requirements ensure that individuals are informed about the third country to which their data will be provided.

Moreover, the controller must not enter into a contract with the third party-recipient in violation of PIPA, which means that the contract must not contain obligations that would contradict the requirements imposed by PIPA on the controller.

The provisions regulating cross-border transfer to an outsourcee or a third party from the Republic of is essentially similar t to the provided under Article 27 of DIFC DP Law 2020.

As the Republic of Korea is a member to the Asia Pacific Economic Cooperation Cross Border Privacy Rules ("APEC CBPR"), if the recipient Organisation holds a "specified certification" that is granted or recognised under the law of that country or territory to which the Personal Data is transferred, the recipient Organisation is taken to be bound by such legally enforceable obligations. Under the Personal Data Protection Regulations 2021, "specified certification" refers to certifications under the APEC CBPR System, and the Asia Pacific Economic Cooperation Privacy Recognition for Processors ("APEC PRP") System. The recipient is taken to satisfy the requirements under the Transfer Limitation Obligation if:

a) it is receiving the Personal Data as an Organisation and it holds a valid APEC CBPR certification; or

b) it is receiving the Personal Data as a data intermediary and it holds either a valid APEC PRP or CBPR certification, or both.

Observation 6: Security of Processing and Breach Reporting

PIPA contains security and breach notifications similar to those found in Article 14, 41 and 42 of the DIFC DP Law 2020.

Security

Personal data controllers must implement technical and administrative measures in accordance with the guidelines prescribed by the Presidential Decree to breach or personal information loss while processing such information. These measures include:

- security measures such as encryption technology and other methods for safe storage and transmission of personal information;
- access controls, such as implementing a system for blocking intrusion to cut off illegal access to personal information as well as measures for preventing alteration of access / log records;
- an internal control plan for safe handling of personal information; and
- anti-virus measures including software, and other protective measures necessary for securing the safety of personal information.

Breach notification

Personal data controller must notify the data subjects without delay of the details and circumstances, and the remedial steps planned. If the number of affected data subjects is 1,000 or more, the personal data controller must also report the notification to data subjects and the result of measures taken to PIPC or the Korea Internet & Security Agency ("KISA")[12]. There is no specific time frame noted for general breaches, only that these actions must be taken without delay and in the latter case, immediately. The remedy process is set out on the PIPC website[13].

Online Service Providers must, under the Network Act, must:

- report a breach to the Ministry of Science and ICT ("MSIT") or KISA within 24 hours of knowledge of the intrusion; and
- analyze causes of intrusion and prevent damage from being spread, whenever an intrusion occurs.

The MSIT may require preservation of data in order to analyze the breach, such as access records of the relevant information and communications network.

[12] *When there is a data breach, the affected Online Service Provider is obligated to provide individual notices to online service users and file a personal information leakage report with the details of the leakage and the remedial steps planned to the PIPC or KISA, regardless of the number of affected data subjects.*

[13] *Remedy procedure: https://www.privacy.go.kr/eng/remedy_01.do There is also a Personal Data Dispute Mediation Committee available for amicable dispute resolution.*

Observation 7:Accountability, Redress and Enforcement

As a means to ensure accountability, Korea requires that anyone who processes personal information directly or indirectly as part of its activities must appoint a privacy officer.

Under the accountability principle in PIPA, entities processing data are required to put in place appropriate technical and organisational measures to effectively comply with their data protection obligations and be able to demonstrate such compliance, in particular to the competent supervisory authority.

According to Article 3(6), (8) PIPA, the personal information controller must process personal information "in a manner to minimise the possibility to infringe" the data subject's privacy, and shall endeavour to obtain the trust of the data subject by observing and performing such duties and responsibilities as provided for in PIPA and other related statutes. This includes the establishment of an internal management plan (Article 29 PIPA) as well as appropriate training and supervision of staff (Article 28 PIPA).

All appointed privacy officers must establish and implement a personal data protection plan; draft up privacy policies; conduct regular surveys on the status and practices of personal data processing, with a view to improve any shortcomings; establish an internal control system to prevent the disclosure, abuse or misuse of personal data; handle complaints and remedial compensation; prepare and implement an education program; protect, control and manage personal data files; and destroying personal data once the purpose of processing has been achieved or the retention period has expired.

In carrying out these duties, the privacy officers may inspect the status of personal data processing and related systems and may request information thereon (Article 31(3) PIPA). If they become aware of any violation of PIPA or other relevant data protection statutes, they shall immediately take corrective measures and report such measures to the management of the controller if necessary. (Article 31(4) PIPA)

Article 31(5) PIPA also provides that a personal information controller must not impose disciplinary measures or disadvantages on the privacy officer without a justifiable ground while performing these functions.

Personal information controllers must also proactively conduct a privacy impact assessment in the case where the operation of personal data files entails a privacy risk, and submit the results thereof to the Protection Commission. (Article 33(8) PIPA)

The result of an impact assessment carried out by a public institution must be communicated to the Personal Information Protection Commission (PIPC) which may provide its opinion and direction where necessary regarding the conditions of processing. (Article 33(1)-(3) PIPA).

Article 13 PIPA provides that the PIPC shall establish policies necessary to promote and support self-regulating data protection activities by controllers, through education and

public relations on the protection of personal information, the promotion and support of agencies and entities involved in protection of personal information, and the introduction and facilitation of a privacy mark system to enhance self-assessment by controllers.

Article 32-2 PIPA, Articles 34-2 to 34-8 of the PIPA Enforcement Decree provides for a follow-up management to ensure that the possibility to certify that a controller's personal data processing and protection system comply with the requirements of PIPA. The principles for accountability set out in PIPA and its Enforcement Decree are equivalent to the required under the DIFC DP Law.

The PIPC has both investigatory and enforcement powers, ranging from recommendations to administrative fines. These powers are further complemented by a regime of criminal sanctions.

The regime in Korea offers various avenues to obtain redress, ranging from low cost options (for instance by contacting the Privacy Call Centre (see footnote 13 above)) to administrative and judicial avenues, including with the possibility to obtain compensation for damages.[14] The redress mechanisms of the Korean system mirror those provided for in Part 9 of the DIFC DP Law 2020. There are further mechanisms available as well where access is necessary for public authorities and national security. This is reflected in DIFC DP Law Article 28, with certain limitations where such processing is necessary and protects data subjects and the public interests.

[14] *EU Adequacy Decision, Section 2.5* https://ec.europa.eu/info/sites/default/files/1_1_180366_dec_ade_kor_new_en.pdf

Observation 8: Additional content principles for specific types of processing (including sharing for the purposes of law enforcement)

As for the obligations of the state, Article 5 of PIPA provides that the government "shall devise policy measures to prevent any harmful effect from collecting personal information for any purpose other than the intended purpose, misusing, abusing, or excessively monitoring and tracking, etc. personal information, thereby protecting human dignity and personal privacy."

Article 15 of PIPA permits collection and use not only with consent but also "where special provisions exist in laws" and "where it is unavoidable so that the public institution may carry out such work under its jurisdiction as stated by laws and regulations". Specific types of processing such as the processing of personal credit information and the processing of network communication data are covered by the Network Act ('ICNA')), and the Use and Protection of Credit Information Act 2009 ("UPCIA") (as amended) regulating personal credit information respectively.

PIPA also contain provisions on special cases such as the processing of pseudonymous data, providing for restrictions on combinations of pseudonymous data, obligations to take safety measures for such data, and on the prohibited acts for the processing of pseudonymised data such as processing to retrieve the identification of an individual. Guidelines are available on the PIPC website[15].

Electronic marketing:

Electronic marketing activities are regulated under the Network Act, which requires the express and prior consent of data subjects for the purpose of electronic direct commercial marketing.

Such consent is not required if a personal information controller has directly collected "contact details" from a data subject, provided them with goods and services and sends them electronic direct marketing for the same kind of goods and services within 6 months of the provision.

For non-electronic direct marketing, such as marketing by post, the data subject's prior consent is required.

This consent requirement is also applicable to direct marketing sent from another jurisdiction to a Korea-based recipient.

[15] *Guidelines for De-identification of Personal Data: https://www.privacy.go.kr/eng/policies_view.do?nttId=8190&imgNo=1*

Observation 9: Existence of International Commitments and Conventions Binding on the Republic of Korea and its Membership in the CBPR System

The Republic of Korea is one of nine APEC economies to have joined the Cross Border Privacy Rules (CBPR) to date — the others include United States, Mexico, Canada, Japan, Singapore, Chinese Taipei, Australia and the Philippines.

The Commissioner's Office also recognizes the CBPR, as set out in the related informational website:

https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system

Conclusion

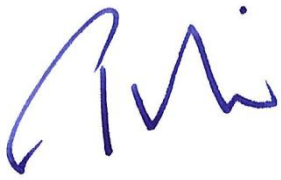
All elements that substantiate recognition of adequacy are generally present. General principles, objectives and functions, accountability, enforcement and supervision, data subjects' rights, the establishment of an independent Commissioner, and other supporting requirements and obligations are essentially the same as the Data Protection Law, DIFC Law No. 5 of 2020.

In addition to the relevant compatible elements of the PIPA and the DIFC DP Law 2020 set out above, the PIPC has demonstrated through available information and documents that it has implemented the PIPA and its relevant updates, and is committed to continuous improvement of inspections, investigations, and supervisory activities. The EU has granted adequacy recognition to the Republic of Korea[16], and the UK is reviewing PIPA alongside the review of other jurisdictions, including the DIFC[17]. Related to this, the Republic of Korea and DIFC Commissioner's Offices share a common objective of reviewing regulatory effectiveness through continuous improvement processes and updates to supervisory activities.

DIFC Commissioner therefore grants provisional adequacy recognition to the Republic of Korea and the CBPR as ensuring adequate data protection in accordance with Article 26 of the DIFC DP Law 2020.

It is recommended that this decision is reviewed and where appropriate reconfirmed on an annual basis. The Commissioner has the right to repeal, amend or suspend this adequacy decision by notification to the Republic of Korea PIPC Commission at any time. This decision shall be reviewed annually.

Dated: February 4, 2022



Jacques Visser
DIFC Commissioner of Data Protection

[16] https://ec.europa.eu/info/files/decision-adequate-protection-personal-data-republic-korea-annexes_en *(please note that relevant limitatations and additional rules and requirements set out in Annexes 1 and 2 of this decision may apply where personal data from the EU is onward transferred from DIFC to South Korea)*

[17] https://www.gov.uk/government/publications/uk-approach-to-international-data-transfers/international-data-transfers-building-trust-delivering-growth-and-firing-up-innovation

Appendix 1: Enforcement Action

Please refer to the following guidance:

Please find reference to recent enforcement decisions:

Cases of Judicial Ruling: https://www.privacy.go.kr/eng/enforcement_01.do

Personal Data Protection-related decisions:
https://www.privacy.go.kr/eng/enforcement_01.do?tabNum=2

Appendix 2: Understanding and Acknowledgement of Article 28 of the DP Law 2020

Article 28 of the DIFC DP Law 2020 states the following:

Data sharing

(1) Subject to any other obligations under this Law and, in particular, a Controller's or Processor's obligations under Part 2 regarding accountability, transparency and compliance with general data protection principles or Part 4 regarding transfers out of the DIFC, where a Controller or Processor receives a request from any public authority over the person or any part of its Group ("a Requesting Authority") for the disclosure and transfer of any Personal Data, it 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 minimise such risks, including by redacting or minimising the Personal Data transferred to the extent possible or utilising appropriate technical or other measures to safeguard the transfer; 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 Part 2 in relation to the Processing of Personal Data by the Requesting Authority.

(2) A Controller or, as applicable, its Processor(s) or any Sub-processor(s), having provided (where possible under Applicable Law) reasonable notice to the Controller, may disclose or transfer Personal Data to the Requesting Authority where it has taken reasonable steps to satisfy itself that:

(a) a request by a Requesting Authority referred to in Article 28(1) is valid and proportionate; and

(b) the Requesting Authority will respect the rights of Data Subjects in the Processing of any Personal Data transferred to it by the Controller pursuant to a request under Article 28(1).

(3) A Controller or Processor may consult with the Commissioner in relation to any matter under this Article 28.

The expectation of the DIFC Commissioner's Office is that these requirements will be considered, and where possible, applied, when relevant entities share Personal Data with government authorities in South Korea.