EUROPEAN
COMMISSION

Brussels, 17.12.2021
C(2021) 9316 final

COMMISSION IMPLEMENTING DECISION

of 17.12.2021

pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the Republic of Korea under the Personal Information Protection Act

(Text with EEA relevance)

COMMISSION IMPLEMENTING DECISION

of 17.12.2021

pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the Republic of Korea under the Personal Information Protection Act

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)[1], and in particular Article 45(3) thereof,

Whereas:

1. INTRODUCTION

(1) Regulation (EU) 2016/679 sets out the rules for the transfer of personal data from controllers or processors in the Union to third countries and international organisations to the extent that such transfers fall within its scope of application. The rules on international data transfers are laid down in Chapter V (Articles 44 to 50) of that Regulation. While the flow of personal data to and from countries outside the European Union is essential for the expansion of cross-border trade and international cooperation, the level of protection afforded to personal data in the Union must not be undermined by transfers to third countries[2].

(2) Pursuant to Article 45(3) of Regulation (EU) 2016/679, the Commission may decide, by means of an implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensure(s) an adequate level of protection. Under this condition, transfers of personal data to a third country may take place without the need to obtain any further authorisation, as provided for in Article 45(1) and recital 103 of Regulation (EU) 2016/679.

(3) As specified in Article 45(2) of Regulation (EU) 2016/679, the adoption of an adequacy decision has to be based on a comprehensive analysis of the third country's legal order, covering both the rules applicable to data importers and the limitations and safeguards as regards access to personal data by public authorities. In its assessment, the Commission has to determine whether the third country in question guarantees a level of protection "essentially equivalent" to that ensured within the European Union (recital 104 of Regulation (EU) 2016/679). Whether this is the case is to be assessed

[1] OJ L 119, 4.5.2016, p. 1.

[2] See recital 101 of Regulation (EU) 2016/679.

against Union legislation, notably Regulation (EU) 2016/679, as well as the case law of the Court of Justice of the European Union[3].

(4) As clarified by the Court of Justice of the European Union, this does not require finding an identical level of protection[4]. In particular, the means to which the third country in question has recourse for protecting personal data may differ from the ones employed in the Union, as long as they prove, in practice, effective for ensuring an adequate level of protection[5]. The adequacy standard therefore does not require a point-to-point replication of Union rules. Rather, the test is whether, through the substance of privacy rights and their effective implementation, supervision and enforcement, the foreign system as a whole delivers the required level of protection[6]. The adequacy referential of the European Data Protection Board, which seeks to further clarify this standard, also provides guidance in this regard[7].

(5) The Commission has carefully analysed Korean law and practice. Based on the findings set out in recitals (8) - (208), the Commission concludes that the Republic of Korea ensures an adequate level of protection for personal data transferred from a controller or processor in the Union[8] to entities (e.g. natural or legal persons, organisations, public institutions) in Korea falling within the scope of application of the Personal Information Protection Act (Act No. 10465 of 29 March 2011, as last amended by Act No. 16930 of 4 February 2020). This includes both controllers and processors (called "outsourcees"[9]) within the meaning of Regulation (EU) 2016/679. The adequacy finding does not cover the processing of personal data for missionary activities by religious organisations and for the nomination of candidates by political parties, or the processing of personal credit information pursuant to the Credit Information Act by controllers that are subject to oversight by the Financial Services Commission.

(6) This conclusion takes into account the additional safeguards set out in Notification No 2021-5 (Annex I) and the official representations, assurances and commitments by the Korean government to the Commission (Annex II).

(7) This Decision has the effect that transfers to controllers and processors in the Republic of Korea may take place without the need to obtain any further authorisation. It does not affect the direct application of Regulation (EU) 2016/679 to such entities where the conditions regarding the territorial scope of that Regulation, laid down in its Article 3, are fulfilled.

2. THE RULES APPLYING TO THE PROCESSING OF PERSONAL DATA

3 See, most recently, Case C-311/18, Facebook Ireland and Schrems (*Schrems II*) ECLI:EU:C:2020:559.

4 Case C-362/14, Maximilian Schrems v. Data Protection Commissioner (*Schrems*), ECLI:EU:C:2015:650, paragraph 73.

5 *Schrems*, paragraph 74.

6 See Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World, COM(2017)7 of 10.1.2017, section 3.1, pp. 6-7.

7 European Data Protection Board, Adequacy Referential, WP 254 rev. 01.available at the following link: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108

8 This Decision has EEA relevance. The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Joint Committee Decision (JCD) incorporating Regulation (EU) 2016/679 into Annex XI of the EEA Agreement was adopted by the EEA Joint Committee on 6 July 2018 and entered into force on 20 July 2018. The Regulation is thus covered by that agreement. For the purposes of the decision, references to the EU and EU Member States should thus be understood as also covering the EEA States.

9 See section 2.2.3 of this Decision.

2.1 The data protection framework in the Republic of Korea

(8) The legal system governing privacy and data protection in Korea has its roots in the Korean Constitution, promulgated on 17 July 1948. While the right to the protection of personal data is not expressly set forth in the Constitution, it is nonetheless recognised as a basic right, derived from the constitutional rights to human dignity and the pursuit of happiness (Article 10), private life (Article 17) and privacy of communications (Article 18). This has been confirmed by both the Supreme Court[10] and the Constitutional Court[11]. Restrictions on fundamental rights and freedoms (including the right to privacy) may only be imposed by law, when necessary for national security or the maintenance of law and order for public welfare, and may not affect the essence of the right or freedom at stake (Article 37(2)).

(9) Even though the Constitution in various places refers to the rights of Korean citizens, the Constitutional Court has ruled that also foreign nationals are the subject of basic rights[12]. In particular, the Court held that the protection of one's dignity and value as a human being, as well as the right to seek happiness, are rights of any human being, not just of citizens[13]. Moreover, according to the official representations from the Korean government[14], it is generally recognised that Articles 12 to 22 of the Constitution (which include privacy rights) provide for basic human rights[15]. Although so far no case law exists specifically regarding the right to privacy of foreign nationals, its grounding in the protection of human dignity and the pursuit of happiness supports this conclusion[16].

(10) Moreover, Korea has enacted a series of laws in the area of data protection that provide safeguards for all individuals, irrespective of their nationality[17]. For the purpose of this Decision, the relevant laws are:

---

10 See, for example, Supreme Court Decision 2014Da77970, 15 October 2015 (English summary available under the link "Lawmaker's disclosure of teachers' trade union members case" at https://www.privacy.go.kr/eng/enforcement_01.do) and the case law cited therein, including Decision 2012Da49933, 24 July 2014.

11 See in particular Constitutional Court Decision 99Hun-ma513, 26 May 2005 (English summary available at http://www.koreanlii.or.kr/w/index.php/99Hun-Ma513?ckattempt=2) and Decision 2014JHun-ma449 2013 Hun-Ba68 (consolidated), 23 December 2015 (English summary available under the link "Change of resident registration number case" at https://www.privacy.go.kr/eng/enforcement_01.do).

12 Constitutional Court Decision 93 Hun-MA120, 29 December 1994.

13 Constitutional Court Decision 99HeonMa494, 29 November 2001.

14 See Section 1.1 of Annex II.

15 See also Article 1 of the Personal Information Protection Act that refers expressly to the "freedoms and rights of individuals". More specifically, it states that the purpose of such Act is "to provide for the processing and protection of personal information for the purposes of protecting [the] freedom and rights of individuals, and further realizing the dignity and value of the individuals." Likewise, Article 5(1) of the Personal Information Protection Act establishes the State's responsibility to "formulate policies to prevent harmful consequences of beyond-purpose collection, abuse and misuse of personal information, indiscrete surveillance and pursuit, etc. and to enhance the dignity of human beings and individual privacy."

16 Moreover, Article 6(2) of the Constitution provides that the status of foreign nationals is guaranteed as prescribed by international law and treaties. Korea is a Party to several international agreements that guarantee the right to privacy, such as the International Covenant on Civil and Political Rights (Article 17), the Convention on the Rights of Persons with Disabilities (Article 22) and the Convention on the Rights of the Child (Article 16).

17 This includes rules that are relevant to the protection of personal data, but do not apply in a situation where personal data is collected in the Union and transferred to Korea under Regulation (EU) 2016/679, for example in the Act on the Protection, Use, etc. of Location Information.

– The Personal Information Protection Act (PIPA);

– the Act on the Use and Protection of Credit Information[18];

– the Communications Privacy Protection Act.

(11) PIPA provides the general legal framework for data protection in the Republic of Korea. It is supplemented by an Enforcement Decree (Presidential Decree No. 23169 of 29 September 2011, last amended by Presidential Decree No. 30892 of 4 August 2020) (PIPA Enforcement Decree), which like PIPA is legally binding and enforceable.

(12) Moreover, regulatory "Notifications" adopted by the Personal Information Protection Commission (PIPC) provide further rules on the interpretation and application of PIPA. Based on Article 5 (Obligations of State) and Article 14 PIPA (International Cooperation), the PIPC adopted Notification No 2021-5 of 1 September 2020 (as amended by No 2021-1 of 21 January 2021 and Notification No 2021-5 of 16 November 2021, Notification No 2021-5) on the interpretation, application and enforcement of certain provisions of PIPA. This Notification provides clarifications that apply to any processing of personal data under PIPA as well as additional safeguards for personal data transferred to Korea based on this Decision. The Notification is legally binding on personal information controllers and enforceable by both the PIPC and courts[19]. A violation of the rules set out in the Notification entails a violation of the relevant provisions of PIPA they complement. The content of the additional safeguards is therefore analysed as part of the assessment of the relevant PIPA articles. Finally, further guidance on PIPA and its Enforcement Decree, which informs the application and enforcement of the data protection rules by the PIPC, is provided in the PIPA Handbook and Guidelines adopted by the PIPC[20].

(13) In addition, the Act on the Use and Protection of Credit Information (CIA) lays down specific rules that apply both to 'ordinary' commercial operators and specialised entities within the financial sector when they process personal credit information, i.e. information that is necessary to determine the creditworthiness of parties to financial or commercial transactions. This includes, in particular, the name, contact details, financial transactions, credit rating, insurance status, or loan balance when such information is used to determine an individual's creditworthiness[21]. Conversely, where such information is used for other purposes (such as human resources), the PIPA applies in its entirety. Concerning the specific data protection provisions of the CIA, compliance is supervised partly by the PIPC (for commercial organisations, see Article 45-3 CIA) and partly by the Financial Services Commission[22] (for the financial sector,

---

18 The purpose of this Act is to foster a sound credit information business, promoting the efficient utilisation and systematic management of credit information, and protecting privacy from the misuse and abuse of credit information (Article 1 of the Act).

19 For example, Korean courts have ruled on compliance with regulatory Notifications in a number of cases, including by holding Korean controllers liable for violations of a Notification (see e.g. Supreme Court Decision 2018Da219406, 25 October 2018, where the Court ordered a controller to pay compensation to individuals for damages suffered because of a violation of the "Notification for the standard for measures to ensure the safety of personal information"; see also Supreme Court Decision 2018Da219352, 25 October 2018; Supreme Court Decision 2011Da24555, 16 May 2016; Seoul Central District Court Decision 2014Gahap511956, 13 October 2016; Seoul Central District Court Decision 2009Gahap43176, 26 January 2010).

20 Article 12(1) PIPA.

21 Article 2(1) CIA.

22 The Financial Services Commission is Korea's supervisory authority for the financial sector and in that capacity also enforces the CIA.

including credit rating agencies, banks, insurance companies, mutual savings banks, specialised credit financial companies, financial investment services companies, securities finance companies, credit unions, etc., see Article 45(1) CIA in conjunction with Article 36-2 CIA Enforcement Decree and Article 38 of the Act on the Financial Services Commission). In this regard, the scope of this Decision is limited to commercial operators that are subject to the oversight of the PIPC[23]. The specific rules of the CIA that apply in this context (the general PIPA rules apply where no specific rules exist) are described in section 2.3.11.

2.2 Material and personal scope of PIPA

(14) Except as otherwise specifically provided for in other Acts, the protection of personal data is governed by PIPA (Article 6). The material and personal scope of its application is determined by the defined concepts of "personal information", "processing" and "personal information controller".

2.2.1 Definition of personal data

(15) Article 2(1) PIPA defines personal information as information relating to a living individual that identifies the individual directly, for instance by his or her name, resident registration number or image, or indirectly, namely where information that cannot by itself identify a certain individual can be easily combined with other information. Whether information can be "easily" combined depends on whether such combination is reasonably likely, taking into account the possibility of obtaining other information as well as the time, cost and technology required to identify an individual.

(16) In addition, pseudonymous information – i.e. information that cannot identify a specific individual without using or combining it with additional information to restore it to its original state – is considered personal data under PIPA (Article 2(1) lit. c) PIPA). Conversely, information that is fully "anonymised" is excluded from the scope of application of PIPA (Article 58-2 PIPA). This is the case for information that cannot identify a specific individual, even if combined with other information, taking into account the time, cost and technology reasonably required for identification.

(17) This corresponds to the material scope of application of Regulation (EU) 2016/679 and its notions of 'personal data', 'pseudonymisation'[24] and 'anonymised information'[25].

---

23 If this would change in the future, e.g. by extending the jurisdiction of the PIPC to all processing of personal credit information under the CIA, it could be considered to amend the adequacy decision to also cover the entities that are currently subject to the oversight of the Financial Services Commission.

24 In PIPA, "pseudonymous processing" is considered processing by methods such as partially deleting personal data or partially or entirely replacing personal data in such a way that no specific individual can be recognised without additional information (Article 2(1-2) PIPA). This corresponds to the definition of pseudonymisation in Article 4(5) Regulation (EU) 2016/679, which refers to "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable person."

25 In particular, recital 26 Regulation (EU) 2016/679 clarifies that the Regulation does not apply to anonymised information, i.e. information that does not relate to an identified or identifiable natural person. This in turn depends on all the means reasonably likely to be used, either by the controller or by another person, to identify the natural person directly or indirectly. To ascertain whether such means are reasonably likely to be used, account must be taken of all objective factors, such as the costs and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.

2.2.2 Definition of processing

(18) The notion of "processing" is broadly defined in PIPA as covering the "collection, generation, connecting, interlocking, recording, storage, retention, value-added processing, editing, retrieval, output, correction, recovery, use, provision, and disclosure, destruction of personal information and other similar activities"[26]. Although certain provisions in PIPA refer only to specific types of processing, such as "use", "provision" or "collection"[27], the notion of "use" is interpreted as including any type of processing other than "collection" or (third-party) "provision". This broad interpretation of "use" thereby ensures that there are no gaps in the protection with respect to specific processing activities. The concept of processing therefore corresponds to the same notion under Regulation (EU) 2016/679.

2.2.3 Personal information controller and "outsourcee"

(19) PIPA applies to "personal information controllers" (controller). Similar to Regulation (EU) 2016/679, this includes any public institution, legal person, organisation or individual that processes personal data directly or indirectly to operate personal data files as part of their activities.[28] In this context, "personal information file" means any "set or sets of personal information arranged or organised in a systematic manner based on a certain rule for easy access to the personal information" (Article 2(4) PIPA)[29]. Internally, the controller is under an obligation to train the persons involved in the processing under its direction, such as company officers or employees, and to exercise appropriate control and supervision (Article 28(1) PIPA).

(20) Specific obligations apply when a controller (the "outsourcer") outsources the processing of personal data to a third party (the "outsourcee"). In particular, the outsourcing must be governed by a legally binding arrangement (typically a contract)[30] that sets out the scope of the outsourced work, the purpose of processing, the technical and managerial safeguards to be applied, supervision by the controller, liability (such as compensation for damages caused by a breach of contractual obligations) as well as

---

26 Article 2(2) PIPA.

27 For example, Articles 15 to 19 PIPA only refer to the collection, use and provision of personal information.

28 Article 2(5) PIPA. Public institutions within the meaning of PIPA include all central administrative departments or agencies and their affiliated bodies, local governments, schools and local government-invested public corporations, the administrative bodies of the National Assembly and the judiciary (including the Constitutional Court) (Article 2(6) PIPA in conjunction with Article 2 PIPA Enforcement Decree).

29 This corresponds to the material scope of application of Regulation (EU) 2016/679. According to Article 2(1) Regulation (EU) 2016/679, the Regulation applies to "the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system." Article 4 lit. 6 Regulation (EU) 2016/679 defines "filing system" as "any structured set of personal data which are accessible according to specific criteria". In line with this, recital 15 explains that the protection of individuals should apply to "the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria, should not fall within the scope of this Regulation."

30 See PIPA Handbook, Chapter III Section 2 on Article 26 (p. 203-212), which explains that Article 26(1) PIPA refers to binding arrangements, such as contracts or similar arrangements.

the limitations to any sub-processing[31] (Article 26(1), (2) PIPA in conjunction with Article 28(1) of the Enforcement Decree)[32].

(21) In addition, the controller has to publish, and continuously update, details on the outsourced work and the identity of the outsourcee, or, to the extent the outsourced processing concerns direct marketing activities, directly notify individuals of the relevant information (Article 26(2), (3) PIPA in conjunction with Article 28(2)-(5) of the Enforcement Decree)[33].

(22) Furthermore, pursuant to Article 26(4) PIPA in conjunction with Article 28(6) of the Enforcement Decree, the controller is under an obligation to "educate" the outsourcee on necessary security measures and supervise, including through inspections, whether it complies with all the controller's obligations under PIPA[34] as well as under the outsourcing contract. Where the outsourcee causes damage due to a violation of PIPA, its actions or failure to act will be attributed to the controller for liability purposes as in the case of an employee (Article 26(6) PIPA).

(23) Although PIPA therefore does not use different concepts for "controllers" and "processors", the rules on outsourcing provide essentially equivalent obligations and safeguards as those regulating the relationship between controllers and processors under Regulation (EU) 2016/679.

2.2.4 Special provisions for information and communication service providers

(24) While PIPA applies to the processing of personal data by any controller, certain provisions contain specific rules (as a *lex specialis*) for the processing of personal data of "users" by "providers of information and communication services"[35]. The notion of "users" covers individuals that use information and communication services (Article 2(1) lit. 4 of the Act on the Promotion of Information and Communications Network Utilisation and Data Protection, Network Act). This requires that the individual either directly uses telecommunication services provided by a Korean telecommunications operator or uses information services[36] provided commercially (i.e. for profit) by an entity that in turn relies on the services of a telecommunications operator licenced/registered in Korea[37]. In both cases, the entity bound by the specific PIPA provisions is one that offers an online service directly to an individual (i.e. a user).

(25) Conversely, an adequacy finding exclusively concerns the level of protection afforded to personal data transferred from a controller/processor in the Union to an entity in a third country (here: the Republic of Korea). In the latter scenario, individuals in the Union will normally have a direct relationship only with the 'data exporter' in the

---

31 According to Article 26(5) PIPA, the processor is prohibited from using any personal information beyond the scope of the outsourced work, or from providing personal information to a third party. Failure to respect this requirement may lead to a criminal sanction pursuant to Article 71 lit. 2 PIPA.

32 Failure to comply with this requirement may lead to the imposition of a fine, see Article 75(4) lit. 4 PIPA.

33 Failure to comply with this requirement may lead to the imposition of a fine, see Article 75(2) lit. 1, (4) lit. 5 PIPA.

34 See also Article 26(7) PIPA, according to which Articles 15 through 25, 27 through 31, 33 through 38, and 50 apply *mutatis mutandis* to the processor.

35 See in particular Article 18(2) and Chapter VI PIPA.

36 Information services comprise both the provision of information and intermediation services for the provision of information.

37 See Article 2(1) lit. 3 (in conjunction with Article 2(1) lit. 2, 4) Network Act and Article 2(6),(8) Telecommunications Business Act.

Union and not with any Korean information and communication service provider[38]. Therefore, the specific provisions of PIPA with respect to personal data of users of information and communication services will, at most, only apply in limited situations to personal data transferred under this Decision.

2.2.5 Exemption from certain provisions of PIPA

(26) Article 58(1) PIPA excludes the application of part of PIPA (i.e. Articles 15 to 57) with respect to four categories of data processing[39]. In particular, the parts of PIPA dealing with the specific grounds for processing, certain data protection obligations, the detailed rules for the exercise of individual rights as well as the rules governing dispute resolution by the Personal Information Dispute Mediation Committee do not apply. Other basic provisions of PIPA remain applicable, in particular the general provisions on data protection principles (Article 3 PIPA) – including for instance the principles of lawfulness, purpose specification and purpose limitation, data minimisation, data accuracy and security – and individual rights (of access, rectification, deletion and suspension, see Article 4 PIPA). In addition, Article 58(4) PIPA imposes specific obligations on those processing activities, namely with respect to data minimisation, limited data retention, security measures and the handling of complaints[40]. As a consequence, individuals could still file a complaint with the PIPC if these principles and obligations would not be respected and the PIPC is empowered to take enforcement action in case of non-compliance.

(27) Firstly, the partial exemption covers personal data collected pursuant to the Statistics Act for processing by public institutions. According to clarifications received from the Korean government, 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

---

38 To the extent that Korean information and communication service providers would have a direct relationship with individuals in the EU (by offering online services), this could lead to the direct application of Regulation (EU) 2016/679, pursuant to its Article 3(2)(a).

39 Article 58(2) PIPA furthermore provides that Articles 15, 22, 27(1) - (2), 34 and 37 do not apply to personal information processed by means of visual data processing devices installed and operated at open places. As this provision concerns the use of video surveillance within Korea, i.e. the direct collection of personal information from individuals in Korea, it is not relevant for the purpose of this Decision, which covers transfers of personal data from controllers/processors in the EU to entities in Korea. In addition, according to Article 58(3) PIPA, Article 15 (collection and use of personal information), Article 30 (obligation to put in place a public privacy policy) and Article 31 (obligation to appoint a privacy officer) do not apply to personal information that is processed to operate groups or associations for friendship (e.g. hobby clubs). Because such groups are considered to be personal in nature, with no connection to a professional or commercial activity, no specific legal basis (such as consent of the individuals concerned) is required in order to collect and use their information in this context. However, all other provisions of PIPA (e.g. data minimisation, purpose limitation, lawfulness of processing, security, and individual rights) continue to apply. Moreover, any processing of the personal information beyond the purpose of establishing a social group would not benefit from the exception.

40 More specifically, Article 58(4) PIPA stipulates an obligation to process personal information to the minimum extent necessary to attain the intended purpose, to process it for a minimum period and to make necessary arrangements for the safe management and appropriate processing of such personal information. The latter includes technical, managerial and physical safeguards, as well as measures to ensure the proper treatment of individual complaints.

public authorities in Korea[41]. Moreover, similar to what is provided in recital 162 of Regulation (EU) 2016/679, the processing of data under the Statistics Act is subject to several conditions and safeguards. In particular, the Statistics Act imposes specific obligations, such as to ensure accuracy, consistency and impartiality; guarantee the confidentiality of individuals; protect the information of respondents to statistical queries including with a view to prevent such information from being used for any other purpose than that of compiling statistic and subject staff members to confidentiality requirements[42]. Public authorities processing statistics must also comply with, inter alia, the principles of data minimisation, purpose limitation and security (Article 3 and 58(4) PIPA) and allow individuals to exercise their rights (of access, correction, deletion and suspension, see Article 4 PIPA). Finally, the data must be processed in an anonymised or pseudonymised form if this allows fulfilling the purpose of processing (Article 3(7) PIPA).

(28) Secondly, Article 58(1) PIPA refers to personal data collected or requested for the analysis of information related to national security. The scope and consequences of this partial exemption are described in more detail in recital (149).

(29) Thirdly, the partial exemption applies to the temporary processing of personal data where this is urgently necessary for reasons of public safety or security, including public health. This category is interpreted strictly by the PIPC and, according to the information received, has never been used. It applies only in emergencies requiring urgent action, for example to track infectious agents, or to rescue and aid victims of natural disasters[43]. Even in those situations, the partial exemption only covers the processing of personal data for a limited time period to carry out such action. Situations where this could apply to data transfers covered by this Decision are even more limited, given the low likelihood that personal data transferred from the Union to Korean operators would be of the type that could render its subsequent processing "urgently necessary" for such emergencies.

(30) Finally, the partial exemption applies to personal data collected or used by the press, for missionary activities by religious organisations, or for the nomination of candidates by political parties. The exemption only applies when personal data is processed by the press, religious organisations or political parties for those specific purposes (i.e. journalistic activities, missionary work and the nomination of political candidates). Where those entities process personal data for other purposes, such as management of human resources or internal administration, PIPA applies in full.

(31) With respect to the processing of personal data by the press for journalistic activities, the balancing between freedom of expression and other rights (including the right to privacy) is provided by the Act on Arbitration and Remedies, etc. for Damage Caused by Press Reports (Press Act)[44]. In particular, Article 5 of the Press Act provides that the press (i.e. any broadcasting organisation, newspaper, periodical or online newspaper), any internet news service, or internet multimedia broadcasting organisation may not infringe the privacy of individuals. If a privacy infringement

---

41 In this respect, Article 33 Statistics Act requires public institutions to protect the information of respondents to statistical queries, including with a view to prevent such information from being used for any other purpose than that of compiling statistics.

42 Article 2(2)-(3), 30(2), 33 and 34 Statistics Act.

43 PIPA Handbook, section on Article 58.

44 For example, Article 4 Press Act provides that press reports must be impartial and objective, in the public interest, respect human dignity and worth, and may neither defame other persons nor infringe on their rights, public morals or social ethics.

nevertheless occurs, it must be remedied promptly in accordance with specific procedures set out in the Act. In this respect, the Act grants individuals that suffer damage due to a press report a number of rights, such as to obtain the publication of a correction of a false statement, a rectification by way of a contradictory statement or a further report (where a press report concerns allegations of crimes of which the individual is later on acquitted)[45]. Claims by individuals may be resolved by press outlets directly (through an ombudsperson)[46], through conciliation or arbitration (before a specialised Press Arbitration Commission)[47] or before the courts. Individuals may also obtain compensation when they suffer monetary damage, infringement of a personality right, or any other emotional distress due to an illegal act of the press (by intention or negligence)[48]. The press is exempt from liability under the Act to the extent that a press report that interferes with the rights of an individual is not contrary to social values and is published either with the consent of the individual concerned, or in the public interest (and there are sufficient grounds to consider that the report corresponds to the truth)[49].

(32) Whereas the processing of personal data by the press for journalistic activities is therefore subject to specific safeguards that follow from the Press Act, there are no such additional safeguards framing the use of the exceptions for the processing activities by religious organisations and political parties in a way comparable to Articles 85, 89 and 91 of Regulation (EU) 2016/679. The Commission therefore considers it appropriate to exclude religious organisations to the extent they process personal data for their missionary activities and political parties to the extent they process personal data in the context of the nomination of candidates from the scope of application of this Decision.

2.3 Safeguards, rights and obligations

2.3.1 Lawfulness and fairness of processing

(33) Personal data should be processed lawfully and fairly.

(34) This principle is laid down by Article 3(1), (2) PIPA and is reinforced by Article 59 PIPA, which prohibits the processing of personal data "by fraud, improper or unjust means", "without legal authority" or "beyond proper authority"[50]. These general

---

45 Articles 15 to 17 Press Act.

46 Every press or media outlet must have its own ombudsperson to prevent and remedy any potential damage caused by the press (e.g. by recommending the correction of press reports that are false or damage the reputation of others), Article 6 Press Act.

47 The Commission consists of between 40 and 90 arbitration commissioners, appointed by the Minister of Culture, Sports and Tourism among persons qualified as judges, attorneys-at-law, persons engaged in news gathering or reporting for at least 10 years, or other persons with expertise related to the press. Arbitration commissioners cannot at the same time be public officials, members of political parties or journalists. In accordance with Article 8 Press Act, arbitration commissioners must carry out their duties independently and may not be subject to any direction or instruction in connection with those duties. Moreover, specific rules are in place to prevent conflicts of interest, e.g. by excluding individual commissioners from handling individual cases where their spouse or relatives are party to the case (Article 10 Press Act). The Commission may handle disputes through conciliation or arbitration, but may also stipulate recommendations to remedy infringements (Section 5 Press Act).

48 Article 30 Press Act.

49 Article 5 Press Act.

50 Article 59 PIPA prohibits any person "who processes or has ever processed personal information" to "acquire personal information or to obtain consent to personal information processing by fraud, improper, or unjust means", "divulge personal information acquired in the course of business, or to provide it for any third party's use without authority" or "damage, destroy, alter, forge, or divulge other's personal information without legal authority or beyond proper authority." A violation of this

principles of lawful processing are elaborated in Articles 15 to 19 PIPA which set out the different legal bases for processing (collection, use and provision to third parties), including the circumstances under which this may involve a change of purpose (Article 18 PIPA).

(35) According to Article 15(1) PIPA, a controller may only collect personal data (within the scope of the purpose of collection) on a limited number of legal grounds. These are (1) the data subject's consent[51] (lit. 1); (2) the necessity to execute and perform a contract with the data subject (lit. 4); (3) a special authorisation in law or necessity for compliance with a legal obligation (lit. 2); the necessity[52] for a public institution to carry out the tasks within its jurisdiction as prescribed by law; (4) the manifest necessity for the protection of the data subject's or a third party's life, body or property interests from imminent danger (only if the data subject is not in a position to express his or her intention, or prior consent cannot be obtained) (lit. 5); (5) the necessity to attain the "justifiable interest" of the controller if it is "manifestly superior" to the interests of the data subject (and only where the processing bears a "substantial relation" to the legitimate interest and does not go beyond what is reasonable) (lit. 6)[53]. These grounds for processing are essentially equivalent to those

---

prohibition may lead to criminal sanctions, see Article 71(5),(6) and Article 72(2) PIPA. Article 70(2) PIPA furthermore allows imposing a criminal penalty for obtaining personal information processed by third parties by fraud or other unjust means or methods, or for providing it to a third party for profit-making or unjust purposes, as well as abetting or arranging such conduct.

51 Consent needs to be freely given, informed, specific, and expressed in one of several ways predetermined by law. In any event, consent may not be obtained by fraud, improper or otherwise unjust means (Article 59(1) PIPA). First, according to Article 4 lit. 2 PIPA, data subjects have the right "to consent or not" and "to elect the scope of consent", and should be informed thereof (Articles 15(2), 16(2),(3), 17(2) and 18(3) PIPA). Article 22(5) PIPA contains a further safeguard by prohibiting a controller from denying the provision of goods or services where this could undermine the individual's free choice in granting consent. This includes situations where only certain types of processing require consent (while others are based on contract) and also covers the further processing of personal data collected in the context of the provision of goods or services. Second, according to Articles 15(2), 17(2), (3) and 18(3) PIPA, when requesting consent the controller must inform the data subject of the "particulars" of the personal data at stake (e.g. that it concerns sensitive data, see Article 17(2) lit. 2(a) PIPA Enforcement Decree), the purpose of processing, the retention period and any recipient of the data. Any such request shall be made "in an explicitly recognisable manner" which distinguishes matters requiring consent from other matters (Article 22(1) to (4) PIPA). Third, Article 17(1) lit. 1-6 of the PIPA Enforcement Decree stipulates the specific methods by which a controller shall obtain consent, such as written consent with the signature of the data subject, or consent by (return) e-mail. While PIPA does not specifically provide individuals with a general right to withdraw consent, individuals instead have a right to obtain suspension of the processing of data concerning them, which when exercised will lead to a termination of processing and deletion of data (see recital 78 on the right to suspension).

52 According to information received from the PIPC, public institutions may only rely on this ground if processing of personal information is unavoidable, i.e. it must be impossible or unreasonably difficult for the institution to carry out its functions without processing the data.

53 Article 39-3 PIPA imposes specific (stricter) obligations on information and communication service providers with respect to the collection and use of personal information of their users. In particular, it requires that the provider obtains consent of the user, after providing information on the purpose of collection/use, the categories of personal information to be collected and the period for which the information will be processed (Article 39-3(1) PIPA). The same applies when any of these aspects change. Failure to obtain consent for the collection of information is subject to criminal sanctions (Article 71(4-5 PIPA). Exceptionally, personal information of users may be collected or used by information and communication providers without obtaining prior consent. This is the case (1) when it is clearly difficult to obtain normal consent for the personal information required to carry out the contract governing the provision of information communications services because of economic and technological reasons (e.g. when personal data is inevitably created in the process of performing a contract, such as billing information, access logs and payment records); (2) where it is necessary for the

laid down in Article 6 of Regulation (EU) 2016/679, including the "justifiable interest" ground that equals the "legitimate interest" ground in Article 6(1) point (f) of Regulation (EU) 2016/679.

(36) Once collected, personal data may be used within the scope of the purpose of collection (Article 15(1) PIPA), or "within the scope reasonably related" to the purpose of collection, taking into account possible disadvantages caused to the data subject and provided the necessary security measures (e.g. encryption) have been adopted (Articles 15(3) PIPA). To determine whether the purpose of use is "reasonably related" to the original collection purpose, the Enforcement Decree sets out specific criteria, which are similar to those of Article 6(4) Regulation (EU) 2016/679. In particular, there must be a considerable relevance to the original purpose; the additional use must be predictable (for instance in light of the circumstances in which the information was collected); and, where possible, the data must be pseudonymised[54]. The specific criteria used by a controller in this assessment must be disclosed in advance in the privacy policy[55]. Moreover, the privacy officer (see recital (94)) is specifically required to review whether further use takes place within those parameters.

(37) Similar (but somewhat stricter) rules apply to the provision of data to a third party. According to Article 17(1) PIPA, the provision of personal data to a third party is allowed on the basis of consent[56] or, within the purpose of collection, where the information has been collected on one of the legal grounds in Article 15 (1) lit. 2, 3, and 5 PIPA. This excludes in particular any disclosure based on the "justifiable interest" of the controller. Beyond this, Article 17(4) PIPA allows third-party provision "within the scope reasonably related" to the purpose of collection, again taking into account possible disadvantages caused to the data subject and provided the necessary security measures (such as encryption) have been adopted. The same factors as the ones described in recital (36) must be taken into account to assess whether the provision is within the scope reasonably related to the purpose of collection and the same safeguards (i.e. with respect to transparency through the privacy policy and the involvement of the privacy officer) apply.

(38) The receipt of personal data by a Korean data controller from the Union is considered a "collection" within the meaning of Article 15 PIPA. Notification No 2021-5 (Section I of Annex I to this Decision) clarifies that the purpose for which the data was transferred by the concerned EU entity constitutes the purpose of collection for the Korean data controller. As a consequence, Korean data controllers receiving personal data from the Union are in principle required to process such information within the scope of the purpose of the transfer, in accordance with Article 17 PIPA.

---

settlement of charges following the provision of information and communication services; or (3) if permitted by other laws (for example, Article 21(1) lit. 6 of the Act on Consumer Protection in Electronic Commerce provides that business operators may collect personal information on legal guardians of a minor to confirm whether valid consent on behalf of the minor has been obtained) (Article 39-3(2) PIPA). In all cases, information and communication providers may not refuse to provide services simply because the user does not provide more personal information than the minimum required (i.e. the information that is necessary to perform the essential elements of the concerned service), see Article 39-3(3) PIPA

54 See Article 14-2 PIPA Enforcement Decree.

55 Article 14-2(2) PIPA Enforcement Decree.

56 Violations of Article 17(1) lit. 1 PIPA may lead to the imposition of criminal sanctions (Article 71(1) PIPA).

(39) Special limitations apply in the event the controller seeks to use the personal data or provide it to a third party for a different purpose than the purpose of collection[57]. According to Article 18(2) PIPA, a private controller may exceptionally[58] use personal data or provide it to a third party for a different purpose: (1) based on the data subject's additional (meaning separate) consent; (2) where this is provided by special statutory provisions; or (3) where this is manifestly necessary for the protection of the data subject's or a third party's life, body or property interests from imminent danger (only if the data subject is not in a position to express his or her intention, and prior consent cannot be obtained)[59].

(40) Public institutions may also use personal data or provide it to a third party for a different purpose in certain situations. This includes cases where it would otherwise be impossible for public institutions to perform their statutory duties as prescribed by law, subject to authorisation of the PIPC. In addition, public institutions may provide personal data to another authority or court, where this is necessary for the investigation and prosecution of crimes or an indictment; for a court to carry out its functions related to ongoing judicial proceedings; or for the enforcement of a criminal penalty, or an order of care or custody[60]. They may also provide personal data to a foreign government or international organisation to comply with a legal obligation following from a treaty or international convention, in which case they also need to comply with the requirements for cross-border data transfers (see recital (90)).

(41) The principles of lawfulness and fairness of processing are therefore implemented in the Korean legal framework in an essentially equivalent way to Regulation (EU) 2016/679, by allowing processing only on the basis of legitimate and clearly defined grounds. Moreover, in all mentioned cases, the processing is only allowed if it is not likely to "infringe unfairly" on the interests of the data subject or a third party, which requires a balancing of interests. In addition, Article 18(5) of PIPA prescribes additional safeguards when the controller provides the personal data to a third party, which may include a request to restrict the purpose and method of use, or to put in place specific security measures. The third party is in turn required to implement the requested measures.

(42) Finally, Article 28-2 PIPA allows the (further) processing of pseudonymised information without the consent of the concerned individual for the purpose of statistics, scientific research[61] and archiving in the public interest, subject to specific

---

57 The "intended purpose" is the purpose for which the information was collected. For example, when the information is collected on the basis of the consent of the individual concerned, the intended purpose is the purpose that is communicated to the individual under Article 15(2) PIPA.

58 Cf. Article 18(1) PIPA. Violations of Article 18(1),(2) may lead to the imposition of criminal sanctions (Article 71(2) PIPA).

59 Use of personal information or its provision to a third party by information and communication service providers for a different purpose than the original one may only take place on the grounds set out in Article 18(2) lit. 1, 2 PIPA (i.e. where additional consent is obtained or where special provisions exist in law). See Article 18(2) PIPA.

60 Except when the processing is necessary for the investigation of crimes, indictment and prosecution, public institutions that use personal information or provide it to a third party for a different purpose than the purpose of collection (for instance where this is specifically permitted by law, or necessary to perform a treaty) are required to publish the legal grounds for processing, its purpose and scope on their website or the Official Gazette and keep records (Article 18(4) PIPA with Article 15 PIPA Enforcement Decree).

61 Scientific research is defined by Article 2(8) PIPA as "research that applies scientific methods, such as technology development and demonstration, fundamental research, applied research and privately funded research." These categories correspond to those set out in recital 159 Regulation (EU) 2016/679.

safeguards. Similar to Regulation (EU) 2016/679[62], PIPA therefore facilitates (further) processing of personal data for such purposes within a framework providing for appropriate safeguards to protect the rights of individuals. Instead of relying on pseudonymisation as a possible safeguard, PIPA imposes it as a pre-condition in order to carry out certain processing activities for the purposes of statistics, scientific research and archiving in the public interest (such as to be able to process the data without consent or to combine different datasets).

(43) Moreover, PIPA imposes a number of specific safeguards, in particular in terms of required technical and organisational measures, record-keeping, limitations on data sharing and addressing possible risks of re-identification. The combination of the various safeguards described in recitals (44) - (48) ensures that the processing of personal data in this context is subject to essentially equivalent protections compared to those that would be required in accordance with Regulation (EU) 2016/679.

(44) Firstly, and most importantly, Article 28-5(1) PIPA prohibits the processing of pseudonymised information with the purpose of identifying a certain individual. If information that could identify an individual would nevertheless be generated while processing pseudonymised information, the controller must immediately suspend the processing and destroy such information (Article 28-5(2) PIPA). Failure to comply with these provisions is subject to administrative fines and constitutes a criminal offence[63]. This means that, even in those situations where it would be *practically* possible to re-identify the individual, such re-identification is *legally* prohibited.

(45) Secondly, when (further) processing pseudonymised information for such purposes, the controller is required to put in place specific technological, managerial and physical measures to ensure the security of the information (including separately storing and managing the information that is necessary to restore the pseudonymised information to its original state)[64]. In addition, records must be kept of the pseudonymised information processed, the purpose of processing, the history of use and any third party recipients (Article 29-5(2) PIPA Enforcement Decree).

(46) Thirdly and lastly, PIPA provides for specific safeguards to prevent the identification of individuals by third parties in the case where the information is shared. In particular, when providing pseudonymised information to a third party for the purpose of statistics, scientific research or archiving in the public interest, controllers may not include information that could be used to identify a specific individual (Article 28-2(2) PIPA)[65].

(47) More specifically, while PIPA allows the combination of pseudonymised information (processed by different controllers) for the purpose of statistics, scientific research or archiving in the public interest, it reserves that power to specialised institutions

---

62 See Articles 5(1)(b) and 89(1)-(2), and recitals 50 and 157 of Regulation (EU) 2016/679.

63 See Articles 28-6(1), 71(4-3) and 75(2) lit.4-4 PIPA.

64 Article 28-4 PIPA and 29-5 PIPA Enforcement Decree. Failure to comply with this obligation is subject to administrative and criminal sanctions, see Articles 73(1) and 75(2) lit. 6 PIPA.

65 Violations of these requirements may lead to the imposition of criminal sanctions (Article 71(2) PIPA). The PIPC immediately started to enforce these new rules, e.g. in its decision of 28 April 2021, where it imposed a fine and corrective measures against a company that, amongst other violations of PIPA, did not comply with the requirement of Article 28-2(2) PIPA, see at https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8

equipped with specific security facilities (Article 28-3(1) PIPA)[66]. When applying for a combination of pseudonymised data, a controller must submit documentation on, amongst others, the data to be combined, the purpose of combination, as well as the proposed security measures for processing the combined data[67]. To allow for the combination, the controller has to send the data to be combined to the specialised institution and provide a "combination key" (i.e. the information that has been used for pseudonymisation) to the Korea Internet and Security Agency[68]. The latter generates "combination key link data" (that allows linking the combination keys of different applicants in order to achieve combination of the datasets) and provides them to the specialised institution[69].

(48) The controller requesting combination may analyse the combined information at the premises of the specialised institution, in a space where specific technical, physical and administrative security measures are applied (Article 29-3 PIPA Enforcement Decree). Controllers that contribute a dataset for such combination may only take the combined data outside the specialised institution following further pseudonymisation or anonymisation of the combined data, and with the approval of that institution (Article 28-3(2) PIPA)[70]. In considering whether or not to grant such approval, the institution will assess the link between the combined data and the purpose of processing and whether a specific security plan has been drawn up for the use of such data[71]. Exporting the combined information outside the institution will not be allowed if the information contains data that would allow identification of an individual[72]. Finally, the combination and release of pseudonymised data by the specialised institution is supervised by the PIPC (Article 29-4(3) PIPA Enforcement Decree).

2.3.2 Processing of special categories of personal data

(49) Specific safeguards should exist where "special categories" of data are being processed.

---

66 To be designated as such a specialised institution (an "Expert Data Combination Agency"), an application must be submitted to the PIPC together with supporting documents detailing inter alia the facilities and equipment put in place to safely combine pseudonymised data and confirming that the applicant employs at least three full-time staff members with qualifications or experience relating to personal data protection (Article 29-2(1)-(2) PIPA Enforcement Decree). Detailed requirements, e.g. with respect to the qualifications of staff, available facilities, security measures, internal policies and procedures, as well as financial requirements are set out in Notification 2020-9 of the PIPC on Combination and Release of Pseudonymised Information (Schedule I). A designation as expert data combination agency may be revoked by the PIPC (after holding a hearing) on certain grounds, e.g. if the agency no longer meets the security standards required for designation, or if a data breach occurred in the context of data combination (Article 29-2(5)-(6) PIPA Enforcement Decree). The PIPC must publish each designation (or revocation of designation) of an Expert Data Combination Agency (Article 29-2(7) PIPA Enforcement Decree).

67 Article 8(1)-(2) of Notification 2020-9 on Combination and Release of Pseudonymised Information.

68 Article 2(3), (6) and Article 9(1) of Notification 2020-9 on Combination and Release of Pseudonymised Information.

69 Article 2(4) and Article 9(2)-(3) of Notification 2020-9 on Combination and Release of Pesudonymised Information. The specialised institution must immediately destroy the combination key link data following combination (Article 9(4) of the Notification).

70 Violations of the requirements for the combination of datasets may lead to the imposition of criminal sanctions (Article 71(4-2) PIPA). See also Article 29-2(4) PIPA Enforcement Decree.

71 The procedure to approve a release of combined data is set out in Article 11 of Notification 2020-9 on Combination and Release of Pseudonymised Information. In particular, the specialised institution must set up a "release review committee", consisting of members with substantial knowledge of and experience with data protection.

72 Article 29-2(4) PIPA Enforcement Decree and Notification No 2020-9, Article 11.

(50) PIPA contains specific rules as regards the processing of sensitive data[73], which is defined as personal data revealing information about the ideology, belief, admission to 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" and has been prescribed as sensitive information by Presidential Decree[74]. According to clarifications received from the PIPC, sexual life is interpreted as also covering the individual's sexual orientation or preferences[75]. Moreover, Article 18 of the Enforcement Decree adds further categories to the scope of sensitive data, in particular DNA information acquired from genetic testing and data that constitutes a criminal history record. The recent amendment of the PIPA Enforcement Decree has further broadened the notion of sensitive data, by also including personal data revealing racial or ethnic origin and biometric information[76]. Following that amendment, the notion of sensitive data under PIPA is essentially equivalent to the one in Article 9 of Regulation (EU) 2016/679.

(51) According to Article 23(1) PIPA and similarly to what is provided under Article 9(1) of Regulation (EU) 2016/679, processing of sensitive data is generally prohibited, unless one of the enumerated exceptions applies[77]. These limit processing to cases where the controller informs the data subject in accordance with Articles 15 and 17 PIPA and obtains separate consent (i.e. separate from the consent for the processing of other personal data), or where the processing is required or permitted by statute. Public authorities may also process biometric information, DNA information acquired from genetic testing, personal information revealing racial or ethnic origin and data that constitutes a criminal history record on those grounds that are exclusively available to them (for instance where necessary for the investigation of crimes or where necessary for a court to proceed with a case)[78]. As such, the legal bases available for the processing of sensitive data are more limited than for other types of personal data, and even more restrictive in Korean law than they are under Article 9(2) of Regulation (EU) 2016/679.

(52) Moreover, Article 23(2) of PIPA – non-compliance with which can lead to sanctions[79] – underlines the particular importance of ensuring appropriate security when handling sensitive data so that it "may not be lost, stolen, divulged, forged, altered, or damaged." While this is a general requirement under Article 29 PIPA, Article 3(4) makes clear that the level of security must be adapted to the type of personal data that is processed, which means that the particular risks involved in the processing of sensitive data must be taken into account. Moreover, data processing shall always be carried out "in a manner to minimize the possibility to infringe" the data subject's privacy, and if possible "in anonymity" (Article 3(6) and (7) PIPA). These requirements are particularly relevant where the processing concerns sensitive data.

---

73 The need to provide specific protections for the processing of sensitive data, such as data concerning health or sexual behaviour, has also been recognised by the Korean Constitutional Court, see Constitutional Court Decision HunMa 1139, 31 May 2007.

74 Article 23(1) PIPA.

75 See also PIPA Handbook, Chapter III Section 2 on Article 23 (p. 157-164).

76 That is, personal information resulting from specific technical processing of data relating to the physical, physiological or behavioural characteristics of an individual for the purpose of uniquely identifying that individual.

77 Non-compliance with these requirements can lead to sanctions pursuant to Article 71 lit. 3 PIPA.

78 Article 18 PIPA Enforcement Decree provides that the categories of data listed there are excluded from the provision of Article 23(1) of the Act when processed by a public institution pursuant to Article 18(2) lit. 5-9 PIPA.

79 See Articles 73 lit. 1 and 75(2) lit. 6 PIPA.

2.3.3 Purpose limitation

(53) Personal data should be collected for a specific purpose and in a manner that is not incompatible with the purpose of processing.

(54) This principle is ensured by Article 3(1) and (2) PIPA, according to which the controller shall "specify and explicit" the purpose of processing, shall process personal data in an appropriate manner necessary for such purpose and shall not use it beyond such purpose. The general principle of purpose limitation is also confirmed in Articles 15(1), 18(1), 19 and – for processors (so-called "outsourcees") – in Article 26(1) lit. 1, (5) and (7) PIPA. In particular, personal data may in principle only be used and provided to third parties within the scope of the purpose for which it was collected (Article 15(1) and 17(1) lit. 2). Processing for a compatible purpose, i.e. "within the scope reasonably related to the initial purpose of the collection", may only take place if it does not negatively affect the data subjects concerned and if necessary security measures (such as encryption) are adopted (Articles 15(3) and 17(4) PIPA). To determine whether further processing is for a compatible purpose, the PIPA Enforcement Decree lists specific criteria that are similar to those provided by Article 6(4) of Regulation (EU) 2016/679, see recital (36).

(55) As explained in recital (38), the purpose of collection in case of Korean controllers receiving personal data from the Union is the purpose for which the data is transferred. A change of purpose by the controller is only allowed exceptionally, in specific (enumerated) cases (Article 18(2) lit. 1-3 PIPA, see also recital (39)). To the extent a change of purpose is authorised by law, such laws in turn have to respect the fundamental right to privacy and data protection, as well as the principles of necessity and proportionality laid down in the Korean Constitution. Moreover, Article 18(2) and (5) PIPA provides for additional safeguards, in particular the requirement that such a change of purpose must not "infringe unfairly on the interest of a data subject", thus always necessitating a balancing of interests. This provides for a level of protection essentially equivalent to that under Article 5(1) lit. b) and Article 6, in conjunction with recital 50, of Regulation (EU) 2016/679.

2.3.4 Data accuracy and minimisation

(56) Personal data should be accurate and, where necessary, kept up to date. It should also be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

(57) The principle of accuracy is similarly recognised in Article 3(3) PIPA, which requires that personal data is "accurate, complete and up to date to the extent necessary in relation to the purposes" for which the data is processed. Data minimisation is required under Articles 3(1), (6) and 16(1) PIPA, which stipulate that the controller shall (only) collect personal data "to the minimum extent necessary" for the intended purpose, and that it bears the burden of proof in this regard. If it is possible to fulfil the purpose of collection by processing information in anonymised form, controllers should endeavour to do so (Article 3(7) PIPA).

2.3.5 Storage limitation

(58) Personal data should in principle be kept for no longer than is necessary for the purposes for which the personal data is processed

(59) The principle of storage limitation is similarly provided by Article 21(1) PIPA[80], which requires the controller to "destroy"[81] personal data without delay upon achievement of the purpose of processing or upon expiry of the retention period (whichever is earlier), unless further retention is required by statute[82]. In the latter case, the relevant personal data "shall be stored and managed separately from other personal information" (Article 21(3) PIPA).

(60) Article 21(1) PIPA does not apply when pseudonymised data is processed for statistical purposes, scientific research or archiving in the public interest[83]. To ensure the principle of limited data retention also in this case, Notification 2021-5 requires controllers to anonymise the information in accordance with Article 58-2 PIPA if the data has not been destroyed upon fulfilment of the specific purpose of processing[84].

2.3.6 Data security

(61) Personal data should be processed in a manner that ensures its security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage. To that end, business operators should take appropriate technical or organisational measures to protect personal data from possible threats. These measures should be assessed taking into consideration the state of the art, related costs and the nature, scope, context and purposes of processing, as well as the risks for the rights of individuals.

(62) A similar principle of security is laid down in Article 3(4) PIPA, which requires controllers to "manage personal information safely according to the processing methods, types, etc. of personal information, taking into account the possibility of infringement on data subject rights and the severity of the relevant risks". Moreover, the controller "shall process personal information in a manner to minimise the possibility to infringe on the privacy of a data subject", and in this context shall endeavour to process personal data in anonymity or in pseudonymised form, if possible (Article 3(6) and (7) PIPA).

(63) These general requirements are further elaborated in Article 29 PIPA, according to which every controller "shall take such technical, managerial and physical measures as establishing an internal management plan and preserving log-on records, etc. that are necessary to ensure safety as prescribed by Presidential Decree so that the personal information may not be lost, stolen, divulged, forged, altered or damaged." Article 30(1) of the PIPA Enforcement Decree specifies those measures by referring to (1) the formulation and implementation of an internal management plan for the safe processing of personal data, (2) access controls and restrictions, (3) the adoption of

---

80 Article 8 (in conjunction with Article 8-2 Enforcement Decree), Article 11 (in conjunction with Article 12(2) Enforcement Decree).

81 On the methods for destroying personal information, see Article 16 PIPA Enforcement Decree. Article 21(2) PIPA clarifies that this shall include "necessary measures to block recovery and revival".

82 Failure to comply with these requirements may lead to criminal sanctions (Article 73(1-2 PIPA). Article 39-6 PIPA imposes an additional requirement on information and communication service providers to delete personal information of users that have not made use of the offered information and communication services for at least one year (unless further retention is required by law or at the request of the individual). Individuals must be informed of the intended deletion of their information 30 days prior to the expiration of the one year deadline (Article 39-6(2) PIPA and Article 48-5(3) PIPA Enforcement Decree). If further retention is required by law, the retained data must be stored separately from other information of users and may only be used or disclosed in accordance with that law (Article 48-5(1)-(2) PIPA Enforcement Decree).

83 Article 28-7 PIPA.

84 Notification 2021-5 (Annex I), Section 4.

encryption technology to safely store and transmit personal data, (4) login records (5) security programs, and (6) physical measures such as a safe storage or locking system[85].

(64) In addition, specific obligations apply if a data breach occurs (Article 34 PIPA in conjunction with Articles 39 and 40 of the PIPA Enforcement Decree)[86]. In particular, the controller is required to notify the aggrieved data subjects of the details of the breach without delay[87], including information about (mandatory) countermeasures taken by the controller and what data subjects can do to minimise the risk of damage (Article 34(1), (2) PIPA)[88]. Where the data breach concerns at least 1,000 data subjects, the controller shall, without delay, also report the data breach and the countermeasures taken to the PIPC and the Korea Internet and Security Agency, which may provide technical assistance (Article 34(3) PIPA in conjunction with Article 39 of the PIPA Enforcement Decree). Controllers are liable for damage resulting from data breaches, in accordance with the provisions of the Civil Act on tort liability (see also section 2.5 on redress)[89].

(65) In complying with its security obligations, the controller must be assisted by a privacy officer, whose tasks include, among others, the building of an internal control system "to prevent the divulgence, abuse and misuse of personal information" (Article 31(2) lit. 4 PIPA). Moreover, the controller has a duty to conduct "appropriate control and supervision" of those of its staff processing personal data, including as regards its safe management; this includes the necessary training ("education") of employees (Article 28(1), (2) PIPA). Finally, in the case of sub-processing, the controller must impose

---

85 With respect to the processing of personal data by information and communication service providers, Article 39-5 PIPA explicitly provides that the number of persons that handle personal information of users shall be limited to the minimum. Moreover, information and communication service providers shall ensure that personal information of users is not exposed to the public through the information and communications network (Article 39-10(1) PIPA). Exposed information must be deleted or blocked at the request of the PIPC (Article 39-10(2) PIPA). More generally, information and communication service providers (and third parties that receive personal data of users) are subject to additional security obligations, specified in Article 48-2 PIPA Enforcement Decree, e.g. the development and implementation of an internal management plan with respect to security measures, measures to ensure access control, encryption, use of software to detect malicious programs, etc.

86 In addition, there is a general prohibition to damage, destroy, alter, forge or leak personal information without legal authority, see Article 59 lit. 3 PIPA.

87 The requirement to notify the individual does not apply to the extent that a data breach occurs with respect to pseudonymised information processed for the purposes of statistics, scientific research or archiving in the public interest (Article 28-7 PIPA, which provides for an exemption from Articles 34(1) and 39-4 PIPA). Ensuring individual notification would require the concerned controller to identify individuals from the pseudonymised dataset, which is expressly prohibited under Article 28-5 PIPA. However, the general data breach notification requirement (to the PIPC) continues to apply.

88 The notification requirements, including its timing and the possibility for a notification "in stages", are further specified in Article 40 of the PIPA Enforcement Decree. Stricter rules apply to information and communication service providers that are required to notify the data subject and the PIPC within 24 hours after becoming aware of the fact that personal information has been lost, stolen or leaked (Article 39-4(1) PIPA). This notification must include details of the personal information that has been leaked, the point in time when this happened, the measures that can be taken by the user, response measures adopted by the provider and the contact details of the department to which the user can address questions (Article 39-4(1)1-5 PIPA). If there is a justifiable reason, e.g. not having the contact details of the user, other means of notification may be used, e.g. by making the information publicly available on a website (Article 39-4(1) PIPA in conjunction with Article 48-4(4) et seq. of the PIPA Enforcement Decree). In that case, the PIPC must be informed of the reasons (Article 34-4(3) PIPA).

89 See e.g. Supreme Court Decisions 2011Da59834, 2011Da59858 and 2011Da59841, 26 December 2012. An English summary is available here: http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm.

requirements on the "outsourcee" among others as regards the safe management of personal data ("technical and managerial safeguards"), and must supervise how these are implemented through inspections (Article 26(1) and (4) PIPA in conjunction with Article 28(1) lit. 3, 4 and (6) of the PIPA Enforcement Decree).

2.3.7 Transparency

(66) Data subjects should be informed of the main features of the processing of their personal data.

(67) This is ensured in different ways in the Korean system. Aside from the right to information pursuant to Article 4 lit. 1 (in general) and Article 20(1) PIPA (for personal data collected from third parties), as well as the right of access pursuant to Article 35 PIPA, PIPA includes a general transparency requirement as regards the purpose of processing (Article 3(1) PIPA) and specific transparency requirements in the case where the processing is based on consent (Articles 15(2), 17(2) and 18(3) PIPA)[90]. Moreover, Article 20(2) PIPA requires certain controllers – those for which processing exceeds certain thresholds[91] – to notify the data subject whose personal data they have received from a third party of the information source, 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. Exceptions apply for certain personal data files held by public authorities, in particular files that contain data processed for national security, other particularly important ("grave") 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 "manifestly superior" to the rights of the data subjects concerned (Article 20(4) PIPA). This requires a balancing of interests.

(68) In addition, Article 3(5) PIPA prescribes that controllers shall make their privacy policy (and other matters related to personal data processing) public. This requirement is further specified in Article 30 PIPA in conjunction with Article 31 of the PIPA Enforcement Decree. According to those provisions, the public privacy policy must among others include (1) the types of personal data processed, (2) the purpose of processing, (3) the retention period, (4) whether personal data is provided to a third party[92], (5) any sub-processing, (6) information on the rights of the data subject and how to exercise them and (7) contact information (including the name of the privacy officer or the internal department responsible for ensuring compliance with the data

---

90 In particular, when personal information is processed with the consent of an individual, the controller must inform the individual of the purpose of processing, details about the information to be processed, the recipient of the information, the period for which personal information is retained and used as well as the fact that the individual is entitled to deny consent (and any disadvantage that may result therefrom).

91 According to Article 15-2(1) PIPA Enforcement Decree, this concerns controllers processing sensitive information of at least 50,000 data subjects, or 'normal' personal information of at least 1 million data subjects. Article 15-2(2) PIPA Enforcement Decree sets out the methods and timing of notification, Article 15-2(3) the requirement to keep certain records thereof. In addition, specific rules apply to certain categories of information and communication service providers (those that generated at least 10 billion won sales revenue during the previous year, or those that store/manage personal data of at least one million users a day on average during the three months preceding the end of the previous year), which are required to notify users of the use history of their personal information on a regular basis, unless this proves impossible due to the lack of any contact information (Article 39-8 PIPA and Article 48-6 PIPA Enforcement Decree).

92 According to the information received from the Korean government, this entails an obligation to list the recipient(s) in the public privacy policy individually.

protection rules and complaint handling). The privacy policy must be made publicly available in such a way that data subjects "may recognise it with ease" (Article 30(2) of PIPA)[93] and must be continuously updated (Article 31(2) of the PIPA Enforcement Decree).

(69) Public institutions are subject to an additional obligation to register, in particular, the following information with the PIPC: (1) the name of the public institution, (2) the grounds and purposes for the processing of the personal data files, (3) the particulars of the personal data that is recorded, (4) the method of processing, (5) the retention period, (6) the number of data subjects whose personal data is retained, (7) the department that handles data subject requests and (8) the recipients of personal data when data is provided routinely or repetitively (Article 32(1) PIPA)[94]. Registered personal data files are made public by the PIPC and must also be referenced by public institutions in their privacy policy (Articles 30(1) and 32(4) PIPA).

(70) To enhance transparency for data subjects in the Union whose personal data is transferred to Korea on the basis of this Decision, Section 3(i) and (ii) of Notification 2021-5 (Annex I) imposes additional transparency requirements. Firstly, when receiving personal data from the Union on the basis of this Decision, Korean controllers must notify the concerned data subjects without undue delay (and in any event not later than one month from the transfer) of the name and contact details of the entities transferring and receiving the information, the personal data (or categories of personal data) transferred, the purpose of collection by the Korean controller, the retention period and the rights available under PIPA. Secondly, when providing personal data received from the Union on the basis of this Decision to third parties, data subjects must be informed inter alia about the recipient, the personal data or categories of personal data to be provided, the country to which the data is provided (where applicable), as well as the rights available under PIPA[95]. This way, the Notification ensures that EU individuals continue to be informed of the specific controllers processing their information and are able to exercise their rights vis-à-vis the relevant entities.

(71) Section 3 (iii) of the Notification (Annex I) allows certain limited and qualified exceptions to these additional transparency obligations that are essentially equivalent to those provided under Regulation (EU) 2016/679. In particular, notification of data subjects in the Union is not required (1) where and as long as it is necessary to restrict notification for certain reasons of public interest (for instance where the information is processed for the purposes of national security or ongoing criminal investigations), to the extent that these public interest objectives are manifestly superior to the rights of the data subject; (2) where the data subject already has the information; (3) where and as long as notification is likely to cause harm to the life or body of the individual or another person, or to unfairly infringe on the property interests of another person, where those rights or interests are manifestly superior to the rights of the data subject; or (4) where there are no contact details for the concerned individuals, or a disproportionate effort would be required to notify them. In determining whether or not it is possible to contact the data subject, or whether this involves excessive efforts,

93 Further modalities are set out in Article 31(3) PIPA Enforcement Decree.

94 The registration requirement does not apply to certain types of personal information files, for example those that record matters related to national security, diplomatic secrets, criminal investigations, prosecution, punishment, investigations of crimes related to taxation, or files that exclusively relate to internal job performance (Article 32(2) PIPA).

95 Notification 2021-5, Section 3 (ii) (Annex I).

the possibility to cooperate with the data exporter in the Union shall be taken into account.

(72) The rules in recitals (67) - (71) therefore ensure an essentially equivalent level of protection with respect to transparency as to what is provided for under Regulation (EU) 2016/679.

2.3.8 Individual rights

(73) Data subjects should have certain rights which can be enforced against the controller or processor, in particular the right of access to data, the right to rectification, the right to object to processing and the right to have data erased. At the same time, such rights may be subject to restrictions, insofar as these restrictions are necessary and proportionate to safeguard important objectives of general public interest.

(74) According to Article 3(5) PIPA, the controller shall guarantee the data subject rights listed in Article 4 PIPA and further specified in Articles 35 to 37, 39 and 39-2 PIPA.

(75) Firstly, individuals have rights to information and access. When the controller has collected personal data from a third party – as will always be the case where the data is transferred from the Union – data subjects generally have the right to receive information on (1) the "source" of the personal data collected (i.e. the transferor), (2) the purpose of processing and (3) the fact that the data subject is entitled to demand suspension of processing (Article 20(1) PIPA). Limited exceptions apply, namely where such 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, but only where these third party interests are "explicitly superior" to the rights of the data subject (Article 20(4) lit. 2 PIPA).

(76) In addition, Article 35(1) and (3) PIPA in conjunction with Article 41(4) of the PIPA Enforcement Decree provides data subjects with the right of access to their personal information[96]. The right of access covers confirmation on the processing, information on the type of data processed, the purpose of processing, the retention period, as well as any disclosure to a third party, and the provision of a copy of the personal information processed (Article 4 lit. 3 PIPA in conjunction with Article 41(1) of the PIPA Enforcement Decree)[97]. Access may be limited (partial access)[98] or denied only where this is provided for by law[99], where it would likely cause damage to the life or body of a third party, or an unjustified infringement of property and other interests of another person (Article 35(4) PIPA)[100]. The latter implies that a balancing should take place between the constitutionally protected rights and freedoms of the individual, on

---

96 According to Article 35(3) PIPA in conjunction with Article 42(2) PIPA Enforcement Decree, the controller may postpone access for "good cause" (i.e. on justified grounds, e.g. if more time is needed to assess whether access can be provided), but must notify the data subject of such justification within 10 days and provide information on how to appeal this decision; as soon as the ground for postponement no longer exists, access must be granted.

97 Access to personal information processed by a public institution may be obtained directly from the institution or indirectly by lodging a request with the PIPC, which shall transmit the request, without delay (Article 35(2) PIPA and Article 41(3) PIPA Enforcement Decree).

98 According to Article 42(1) PIPA Enforcement Decree, the controller is under an obligation to grant partial access where at least part of the information is not covered by the grounds for refusal.

99 Such law must in turn respect the fundamental right of privacy and data protection, as well as the principles of necessity and proportionality laid down in the Korean Constitution.

100 In addition, public institutions may refuse to grant access if doing so would cause grave difficulties in carrying out certain functions, including ongoing audits or the imposition, collection or repayment of taxes (Article 35(4) PIPA).

the one hand, and of other persons, on the other hand. Where access is limited or denied, the controller must notify the data subject of the grounds therefor and how to appeal the decision (Articles 41(5), 42(2) of the PIPA Enforcement Decree).

(77) Secondly, data subjects have the right to the correction or erasure[101] of their personal data, "unless otherwise specifically provided by other statutes" (Article 36(1) and (2) PIPA)[102]. Upon receipt of a request, the controller must investigate the matter without delay, take the necessary measures[103] and notify the data subject thereof within 10 days; where the request cannot be granted, this notification requirement covers the reasons for the denial and how to appeal (see Article 36(4) PIPA in conjunction with Article 43(3) of the PIPA Enforcement Decree)[104].

(78) Finally, data subjects have the right to the suspension of processing of their personal data, without delay[105], unless one of the enumerated exceptions apply (Article 37(1), (2) PIPA)[106]. The controller may deny the request (1) where this is specifically authorised by law or necessary ("inevitable") to comply with legal obligations, (2) where suspension would likely cause damage to the life or body of a third party, or an unjustified infringement of property and other interests of another person, (3) where it would be impossible for a public institution to carry out its function as prescribed by law without processing the information, or (4) where the data subject fails to expressly terminate the underlying contract with the controller even though it would be impracticable to perform the contract without such data processing. In this case, the controller must, without delay, notify the data subject of the reasons for denial and how to appeal (Article 37(2) PIPA in conjunction with Article 44(2) of the PIPA Enforcement Decree). According to Article 37(4) PIPA, the controller must, without delay, "take necessary measures including destruction of the relevant personal information" when complying with the suspension request[107].

(79) The right to suspension also applies where personal data is used for direct marketing purposes, i.e. in order to promote goods or services, or solicit the purchase thereof. Moreover, such further processing generally requires the specific (additional) consent of the data subject (see Article 15(1) lit. 1, Article 17(2) lit. 1 of PIPA)[108]. When requesting this consent the controller must inform the data subject in particular of the

---

101 In this case, the controller must take measures preventing recovery of the personal information, see Article 36(3) PIPA.

102 Such statutes must meet the requirements of the Constitution that a fundamental right may only be restricted when necessary for national security, or the maintenance of law and order for public welfare, and may not affect the essence of the freedom or right (Article 37(2) of the Constitution).

103 Article 43(2) PIPA Enforcement Decree provides for a special procedure in case the controller processes personal information files provided by another controller.

104 Failure to take the necessary measures to correct or erase personal information and continuous use or provision of that information to a third party may lead to criminal sanctions (Article 73(2) PIPA).

105 According to Article 44(2) PIPA Enforcement Decree, the controller shall inform the data subject of the fact that it has duly suspended the processing within 10 days from the receipt of the request.

106 With respect to public institutions, the right to the suspension of processing may be exercised with respect to information contained in registered personal information files (Article 37 in conjunction with Article 32 PIPA). Such registration is not required in a limited number of situations, e.g. where the personal information files relate to national security, criminal investigations, diplomatic relations, etc. (Article 32(2) PIPA).

107 Failure to suspend the processing may lead to criminal sanctions (Article 73(3) PIPA).

108 The Dispute Mediation Committee (see recital 133) has dealt with several cases where individuals complained about the use of their data for direct marketing purposes without consent, which have for instance led to the payment of compensation and deletion of personal data by the relevant controller (see e.g. Dispute Mediation Committee 20R10-024(2020.11.18), 20R08-015(2020,8,28), 20R07-031(2020.9.1)).

intended use of the data for direct marketing purposes – i.e. the fact that (s)he may be contacted to promote goods or services or solicit the purchase thereof – in an "explicitly recognisable manner" (Article 22(2), (4) of PIPA in conjunction with Article 17(2) lit. 1 of the PIPA Enforcement Decree).

(80) In order to facilitate the exercise of individual rights, the controller must establish dedicated procedures and publicly announce them (Article 38(4) PIPA).[109] This includes procedures for raising objections against the denial of a request (Article 38(5) PIPA). The controller must ensure that the procedure for exercising rights is "data-subject friendly" and not more difficult than the one for the collection of the personal data; this also includes the obligation to provide information on the procedure on its website (Articles 41(2), 43(1) and 44(1) of the PIPA Enforcement Decree).[110] Individuals may authorise a representative to file such a request (Article 38(1) PIPA in conjunction with Article 45 of the PIPA Enforcement Decree). While the controller is entitled to impose a fee (and, in case of a request to mail copies of personal data, postage), the amount has to be determined "within the actual expenses necessary for the processing of [the request]"; no fee (nor postage) may be imposed where the controller has caused the request (Article 38(3) PIPA in conjunction with Article 47 of the PIPA Enforcement Decree).

(81) PIPA and its Enforcement Decree do not contain general provisions addressing the issue of decisions affecting the data subject and based solely on the automated processing of personal data. However, as regards personal data that has been collected in the Union, any decision based on automated processing will typically be taken by the controller in the Union (which has a direct relationship with the concerned data subject) and is thus subject to Regulation (EU) 2016/679.[111] This includes transfer scenarios where the processing is carried out by a foreign (for instance Korean) business operator acting as an agent (processor) on behalf of the controller in the Union (or as a sub-processor acting on behalf of the Union processor having received the data from a Union controller that collected it) which on this basis then takes the decision. Therefore, the absence of specific rules on automated decision-making in the PIPA is unlikely to affect the level of protection of the personal data transferred under this Decision.

(82) As an exception, the provisions of regarding transparency on request (Article 20) and individual rights (Articles 35 to 37), as well as the individual notification requirement for information and communication service providers (Article 39-8 PIPA), do not apply with respect to pseudonymised information, when this is processed for the purpose of statistics, scientific research or archiving in the public interest (Article 28-7 PIPA)[112]. In line with the approach of Article 11(2) (in conjunction with recital 57) of Regulation (EU) 2016/679, this is justified by the fact that, to ensure transparency or grant individual rights, the controller would have to identify whether any (and if so

---

109 See also Article 30(1) lit. 5 PIPA on the privacy policy, which among others shall contain information on the rights available to the individual and how to exercise them.

110 See also Article 39-7(2) PIPA with respect to information and communication service providers.

111 Conversely, in the exceptional case where the Korean business operator has a direct relationship with the EU data subject, this will typically be a consequence of it having targeted the individual in the European Union by offering him or her goods or services or monitoring his or her behaviour. In this scenario, the Korean business operator will itself fall within the scope of application of the Regulation (EU) 2016/679 (Article 3(2)) and thus has to directly comply with EU data protection law.

112 See also Notification 2021-5, which confirms that Section III PIPA (including Article 28-7) only applies when pseudonymised information is processed for scientific research, statistics or archiving in the public interest, see Section 4 of Annex I to this Decision.

which) data is related to the individual making the request, which is expressly prohibited under PIPA (Article 28-5(1) PIPA). Moreover, where such re-identification involves undoing the pseudonymisation for the entire (pseudonymised) dataset, it would expose the personal information of all other individuals concerned to increased risks.. Whereas Regulation (EU) 2016/679 refers to situations where re-identification is practically impossible, PIPA adopts a stricter approach by expressly prohibiting re-identification in all situations where pseudonymised information is processed.

(83) The Korean system, as described in recitals (74) - (82), therefore contains rules on data subject rights that provide a level of protection essentially equivalent to that under Regulation (EU) 2016/679.

2.3.9 Onward transfers

(84) The level of protection afforded to personal data transferred from the Union to controllers in the Republic of Korea must not be undermined by the further transfer of such data to recipients in a third country.

(85) Such "onward transfers", constitute international transfers from the Republic of Korea from the perspective of the Korean controller. In this respect, PIPA distinguishes between the outsourcing of processing to an outsourcee (i.e. a processor) and the provision of personal data to third parties[113].

(86) Firstly, 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). 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 (see Article 26(1) PIPA); 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[114] as well as the outsourcing contract.

(87) If the outsourcee causes damage by processing the personal data in violation of PIPA, this will be attributed to the controller for liability purposes, as would be the case with the controller's employees (Article 26(6) PIPA). The Korean controller therefore remains responsible for the personal data that has been outsourced and must ensure that the overseas processor processes the information in accordance with PIPA. 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

---

113 Specific rules apply to information and communication service providers. In accordance with Article 39-12 PIPA, information and communication service providers must in principle 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 (1) the particulars of the information to be transferred, (2) the country to which the information will be transferred (as well as the date and method of the transfer), (3) the name of the recipient and (4) the purpose of use and retention by the recipient (Article 39-12(3) PIPA). 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).

114 See also Article 26(7) PIPA, according to which Articles 15 to 25, 27 to 31, 33 to 38, and 50 apply *mutatis mutandis* to the processor.

actions of the outsourcee ensure continuity of protection when personal data processing is outsourced to an entity outside of Korea.

(88) Secondly, Korean 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[115] has to obtain the data subject's consent[116] after having provided the data subject with information on (1) the type of personal data, (2) the recipient of the personal data, (3) the purpose of transfer in the sense of the purpose of processing pursued by the recipient, (4) the retention period for processing by the recipient as well as (5) the fact that the data subject may deny consent (Article 17(2), (3) PIPA). Notification 2021-5, in its section on transparency (see recital (70)), requires that individuals are informed about the third country to which their data will be provided. This ensures that data subjects in the Union can take a fully informed decision on whether or not to consent to an overseas provision. 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[117].

(89) Without the individual's consent, personal data may be provided to a third party (overseas) where the purpose of disclosure remains "within the scope reasonably related" to the initial purpose of collection (Article 17(4) PIPA, see recital (36)). However, in deciding whether (or not) to disclose personal data for a "related" purpose, the controller must take into consideration whether the disclosure causes disadvantages to the individual and whether necessary security measures (such as. encryption) have been taken. Given that the third country to which personal data is transferred may not offer protections similar to those provided under PIPA, Section 2 of Notification 2021-5 recognises that such disadvantages may arise and can only be avoided if the Korean controller and the overseas recipient, through a legally binding instrument (such as a contract), ensure a level of protection equivalent to PIPA, including with respect to data subject rights.

(90) Special rules apply to "out-of-purpose" disclosure, i.e. provision of data to a third party for a new (unrelated) purpose, which may only take place on one of the grounds of Article 18(2) PIPA, as described in recital (39). However, even under those conditions third-party provision is excluded if it is likely to "unfairly infringe" the interests of the data subject or a third party, which requires a balancing of interests. In addition, under Article 18(5) PIPA, the controller must apply additional safeguards, which may include requesting the third party to restrict the purpose and method of processing, or to put in place specific security measures. Again, given that the third country to which personal data is transferred may not offer protections similar to those provided under PIPA, Section 2 of Notification 2021-5 recognises that such an "unfair infringement" of the interests of the individual or a third party may arise and can only be avoided if the Korean controller and the overseas recipient, through a legally binding instrument (such as a contract), ensure a level of protection equivalent to PIPA, including with respect to data subject rights.

---

115 In case of the third-party provision of personal information of users by information and communication service providers, this always requires the consent of the user (Article 39-12(2) PIPA).

116 As explained in more detail in footnote 51, for such consent to be valid, it needs to be freely given, informed and specific.

117 See also Article 39-12(1) PIPA with respect to information and communication service providers.

(91) The rules in recitals (86) - (90) therefore ensure continuity of protection when personal data is onward transferred (to an "outsourcee" or a third party) from the Republic of Korea in a way that is essentially equivalent to what is provided under Regulation (EU) 2016/679.

2.3.10 Accountability

(92) Under the accountability principle, 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.

(93) According to Article 3(6), (8) PIPA, the controller must process personal data "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).

(94) As a means to ensure accountability, Article 31 PIPA in conjunction with Article 32 of the PIPA Enforcement Decree creates an obligation for controllers to designate a privacy officer that "comprehensively takes charge of personal information processing". In particular, such privacy officer is tasked to perform the following functions: (1) establishing and implementing a personal data protection plan and drawing up of the privacy policy, (2) conducting regular surveys on the status and practices of personal data processing, with a view to improve any shortcomings, (3) complaint-handling and remedial compensation, (4) establishing an internal control system to prevent the disclosure, abuse or misuse of personal data, (5) preparing and implementing an education program, (6) protecting, controlling and managing personal data files, and (7) destroying personal data once the purpose of processing has been achieved or the retention period has expired. In carrying out these duties, the privacy officer may inspect the status of personal data processing and related systems and may request information thereon (Article 31(3) PIPA). If the privacy officer becomes aware of any violation of PIPA or other relevant data protection statutes, (s)he shall immediately take corrective measures and report such measures to the management ("head") of the controller, if necessary (Article 31(4) PIPA). According to Article 31(5) PIPA, the privacy officer must not suffer unjustified disadvantages as a consequence of performing these functions.

(95) In addition, controllers must proactively endeavour to conduct a privacy impact assessment in the case where the operation of personal data files entails a privacy risk (Article 33(8) PIPA). Based on Article 33(1), (2) PIPA in conjunction with Articles 35, 36 and 38 of the PIPA Enforcement Decree, factors such as the type and nature of the data processed (in particular whether it constitutes sensitive information), its volume, the retention period, and the likelihood of data breaches will be relevant in assessing the degree of risk to the rights of data subjects. The purpose of the privacy impact assessment is to ensure that the privacy risk factors as well as any safety or other countermeasures are analysed, and to indicate matters that need improvement (see Article 33(1) PIPA in conjunction with Article 38 of the PIPA Enforcement Decree).

(96) Public institutions are under an obligation to carry out an impact assessment when processing certain personal data files which present a higher risk for possible privacy violations (Article 33(1) PIPA). In accordance with Article 35 of the PIPA

Enforcement Decree, this is the case, among others, for files that contain sensitive information on at least 50,000 data subjects, files that will be matched with other files and as a result thereof will contain information on at least 500,000 data subjects, or files that contain information on at least one million data subjects. The result of an impact assessment carried out by a public institution must be communicated to the PIPC (Article 33(1) PIPA), which may provide its opinion (Article 33(3) PIPA).

(97) Finally, Article 13 PIPA provides that the PIPC shall establish policies necessary to promote and support "self-regulating data protection activities" by controllers, among others through education on data protection, the promotion of and support for organisations engaged in data protection, and by assisting controllers in establishing and implementing self-regulatory rules. Moreover, it shall introduce and facilitate the ePRIVACY Mark system. In this respect, Article 32-2 PIPA in conjunction with Articles 34-2 to 34-8 of the PIPA Enforcement Decree provides for the possibility to certify that a controller's personal data processing and protection system(s) comply with the requirements of PIPA. According to these rules, a certification[118] may be granted (for a period of 3 years) if the controller satisfies the certification criteria determined by the PIPC, including the establishment of managerial, technical and physical safeguards to protect personal data[119]. The PIPC must examine the controller's systems relevant for the certification at least once per year to maintain its effectiveness, which can lead to the revocation of the certification (Article 32(4) PIPA in conjunction with Article 34-5 of the PIPA Enforcement Decree; so-called "follow-up management").

(98) The Korean framework therefore implements the principle of accountability in a way that ensures a level of protection essentially equivalent to that under Regulation (EU) 2016/679, including by providing for different mechanisms to ensure and demonstrate compliance with PIPA.

2.3.11 Special rules for the processing of personal credit information

(99) As described in recital (13), the CIA lays down specific rules for the processing of personal credit information by commercial operators. When processing personal credit information, commercial operators therefore need to comply with the general requirements of PIPA, unless the CIA contains more specific rules. This will for example be the case when they process information related to a credit card or bank account in the context of a commercial transaction with an individual. As sectoral legislation for the processing of credit information (both personal and non-personal), the CIA not only imposes specific data protection safeguards (for instance in terms of transparency and security), but also more generally regulates the specific circumstances in which personal credit information may be processed. This is, in particular, reflected in the detailed requirements for the use, the provision of data to a third party and retention of such data.

(100) Like PIPA, the CIA reflects the principle of lawfulness and proportionality. Firstly, as a general requirement, Article 15(1) CIA only allows the collection of personal credit information by reasonable and fair means and to the smallest extent necessary to serve

---

118 In addition, if the controller intends to refer to, or promote, the certification in its business operations, it may use the personal information protection mark established by the PIPC. See Article 34-7 PIPA Enforcement Decree.

119 Since November 2018, the "Personal Information & Information Security Management System" (ISMS-P) has been developed, which certifies that controllers are operating a comprehensive management system.

a specified purpose, in accordance with Article 3(1)-(2) PIPA. Secondly, the CIA specifically regulates the lawfulness of processing of personal credit information, by restricting its collection, use and provision to a third party and generally tying those processing activities to the requirement of consent of the person concerned.

(101) Personal credit information may be collected based on one of the grounds provided by PIPA or on specific grounds set out in the CIA. Given that Article 45 of Regulation (EU) 2016/679 presupposes a transfer of personal data by a controller or processor in the Union, but does not cover direct collection (such as from the individual or a website) by a controller in Korea, only consent and the grounds available under PIPA are relevant for this Decision. Those grounds include, in particular, scenarios where the transfer is necessary to perform a contract with the individual or for the legitimate interests of the Korean controller (Article 15(1) lit. 4, 6 PIPA)[120].

(102) Once collected, personal credit information may be used (1) for the original purpose for which it was (directly) provided by the individual[121]; (2) for a purpose that is compatible with the original purpose of collection[122]; (3) to determine whether to establish or maintain a commercial relationship requested by the individual[123]; (4) for the purpose of statistics, research and archiving in the public interest[124] if the information is pseudonymised[125]; (5) if further consent is obtained or (6) in accordance with the law.

(103) If a commercial operator intends to disclose personal credit information to a third party, it must obtain the individual's consent[126] after informing the individual of the

---

120 The CIA also contains other legal bases for collection, i.e. where required by law, where the information is made public by a public institution pursuant to freedom of information legislation, or where the information is available on a social network. In order for the commercial operator to rely on the last ground, it must be able to show that the collection stays within the scope of the data subject's consent, based on a reasonable ("objective") interpretation and taking into account the nature of the data, the intent and purpose of making it available on the social network, whether the purpose of collection is "highly relevant" to that purpose, etc. (Article 13 CIA Enforcement Decree). However, as explained in recital (101), these grounds will in principle not be relevant in a transfer scenario.

121 For example, when credit information is generated/provided in the context of a commercial transaction with the individual. However, this ground cannot be relied on to use personal credit information for direct marketing purposes (see Article 33(1) lit. 3 CIA).

122 To determine whether the purpose of use is compatible with the original purpose of collection, the following factors must be taken into account: (1) the relationship ("relevance") between the two purposes; (2) the manner in which the information was collected; (3) the impact of the use on the individual and (4) whether appropriate security measures, such as pseudonymisation, have been implemented (cf. Article 32(6) lit. 9-4 CIA).

123 For example, a controller may have to take into account personal credit information it has received from an individual in order to decide whether to extend the term of a loan to that individual.

124 Article 33 CIA, in conjunction with Article 32(6) lit. 9-2, 9-4 and 10 CIA.

125 Pseudonymisation is defined by Article 2(15) CIA as processing personal credit information in such a way that individuals can no longer be identified from the information other than in combination with additional information. Although the CIA contains specific safeguards for the processing of pseudonymised information for the purpose of statistics, research and archiving in the public interest (Article 40-2 CIA), these rules do not apply to commercial organisations. Instead, the latter remain subject to the specific requirements of Section III PIPA, as described in recitals (42)-(48). Article 40-3 CIA furthermore exempts the processing of pseudonymised credit information – where this takes place for purposes of statistics, scientific research or archiving in the public interest – from requirements on transparency and individual rights, similar to the exception in Article 28-7 PIPA and subject to the safeguards of Section III PIPA, as described in more detail in recitals (42)-(48).

126 This does not apply where the information is provided to a third party to keep personal credit information accurate and up to date, as long as the provision remains within the original purpose of processing (Article 32(1) CIA). This may for example occur where up to date information is provided to a credit rating agency to ensure that its records are accurate.

recipient of the data, the purpose of processing by the recipient, the details of the data to be provided, the period of storage by the recipient and the right to refuse consent (Article 32(1) CIA and Article 28(2) CIA Enforcement Decree)[127]. This consent requirement does not apply in specific situations, namely where personal credit information is disclosed[128]: (1) to an outsourcee for outsourcing purposes[129]; (2) to a third party in case of a business transfer, division or merger; (3) for the purpose of statistics, research and archiving in the public interest, where the information is pseudonymised; (4) for a purpose that is compatible with the original purpose of collection; (5) to a third party that uses the information to collect a debt owed by the individual[130]; (6) to comply with a court order; (7) to a prosecutor/judicial police officer in an emergency where the individual's life is in danger or (s)he is expected to suffer bodily injury and no time is available to issue a judicial warrant[131]; (8) to competent tax authorities to comply with taxation laws; or (9) in accordance with other laws. In case of disclosure on one of these grounds, the data subject must be notified thereof in advance (Article 32(7) CIA).

(104) The CIA also specifically regulates the duration of processing of personal credit information on the basis of one of those grounds for use or provision to a third party after the end of the commercial relationship with the individual[132]. Only information that was necessary to establish or maintain that relationship may be retained, subject to additional safeguards (it must be kept separately from credit information that relates to individuals with whom a commercial relationship is ongoing, protected by specific security measures and only accessible by authorised individuals)[133]. All other data must be deleted (Article 17-2(1) lit. 2 CIA Enforcement Decree). To determine which data was necessary for the commercial relationship, different factors must be taken into account, including whether it would have been possible to establish the relationship without the data and whether it directly relates to the goods or services provided to the individual (Article 17-2(2) CIA Enforcement Decree).

(105) Even in cases where personal credit information may in principle be kept beyond the end of the commercial relationship, it must be deleted within three months after achieving the further purpose of processing[134] or, in any event, after five years (Article 20-2 CIA). In a limited number of circumstances, personal credit information may be kept for longer than five years, in particular where necessary to comply with a legal

---

127 If it is impractical to provide the abovementioned information, it may be sufficient to refer the individual to the third-party recipient for the required information.

128 Given that the CIA does not specifically regulate overseas disclosures of personal credit information, such disclosures have to comply with the safeguards for onward transfers imposed by Section 2 of Notification No 2021-5.

129 Outsourcing of the processing of personal credit information may only take place based on a written contract and in accordance with the requirements of Article 26(1)-(3), (5) PIPA, as described in recital (20) (Article 17 CIA and Article 14 CIA Enforcement Decree). The outsourcee may not use the information beyond the scope of the outsourced duties and the outsourcing company must put in place specific security requirements (e.g. encryption) and educate the outsourcee on how to prevent the credit information from being lost, stolen, disclosed, altered or compromised.

130 See also Article 28(10) lit. 1, 2 and 6 CIA Enforcement Decree.

131 In that case, a warrant must be requested without delay. If the warrant is not issued within 36 hours, the received data must be deleted without delay (Article 32(6) lit. 6 CIA).

132 For example because contractual obligations have been fulfilled, one of the parties exercised his/her right to termination, etc., see Article 17-2(5) CIA Enforcement Decree.

133 Article 20-2(1) CIA and Article 17-2(1)lit. 1 CIA Enforcement Decree.

134 This period takes into account that deletion will often not be possible immediately but typically requires certain steps (e.g. separating the data to be deleted from other data and performing the deletion without affecting the stability of information systems) that take some time for implementation.

obligation; where necessary for the vital interests of an individual's life, body or property; for the archiving of pseudonymised information (that was used for purposes of scientific research, statistics or archiving in the public interest); or for insurance purposes (in particular for insurance payments or to prevent insurance fraud)[135]. In these exceptional cases, specific safeguards apply (such as notification of the individual of the further use, separating the retained information from the information that relates to individuals with whom there is still a commercial relationship, limiting access rights, see Article 17-2(1)-(2) CIA Enforcement Decree).

(106) The CIA also further specifies the principles of accuracy and data quality, by requiring that personal credit information is "registered, modified and managed" to keep it accurate and up to date (Article 18(1) CIA and Article 15(3) CIA Enforcement Decree)[136]. When providing credit information to certain other entities (such as credit rating agencies), commercial operators are also specifically required to verify the accuracy of the information to ensure that only accurate information is registered and managed by the recipient (Article 15(1) CIA Enforcement Decree, in conjunction with Article 18(1) CIA). More generally, the CIA requires records to be kept on the collection, use, third party disclosure and destruction of personal credit information (Article 20(2) CIA)[137].

(107) Furthermore, the processing of personal credit information is subject to specific requirements with respect to data security. In particular, the CIA requires the implementation of technological, physical and organisational measures to prevent unlawful access to computer systems as well as the alteration, destruction or any other risk to the processed data (for instance by means of access controls, see Article 19 CIA and Article 16 CIA Enforcement Decree). In addition, when exchanging personal credit information with a third party, an agreement must be concluded that lays down specific security measures (Article 19(2) CIA). If a breach of personal credit information occurs, measures to minimise any damage must be taken and the concerned individuals must be notified without delay (Article 39-4(1)-(2) CIA). In addition, the PIPC must be informed about the notification provided to individuals and the measures that have been implemented (Article 39-4(4) CIA).

(108) The CIA also imposes specific transparency obligations when obtaining consent for the use or provision of personal credit information (Article 32(4) and Article 34-2 CIA and Article 30-3 CIA Enforcement Decree) and, more generally, before providing information to a third party (Article 32(7) CIA)[138]. In addition, individuals have a right to obtain information upon request about the use and provision of their credit

---

135 Article 20-2(2) CIA.

136 Article 18(2) CIA and Article 15(4) CIA Enforcement Decree lay down more specific rules with respect to this record-keeping requirement, e.g. for records concerning information that may disadvantage an individual, such as information on delinquency and bankruptcy.

137 As regards other accountability mechanisms, the CIA requires certain organisations (e.g. cooperatives and public corporations, see Article 21(2) CIA Enforcement Decree) to appoint a "credit information administrator/guardian" who is in charge of monitoring compliance with the CIA and performs the tasks of the "privacy officer" under PIPA (Article 20(3) and (4) CIA).

138 This includes a general notification requirement (Article 32(7) CIA) and a specific transparency obligation in case information by which the credit-worthiness of an individual can be determined is provided to certain entities, such as credit rating agencies and credit information collection agencies (Article 35-3 CIA and Article 30-3 CIA Enforcement Decree), or where a commercial transaction relationship is refused or terminated on the basis of personal credit information received from a third party (Article 36 CIA and Article 31 CIA Enforcement Decree).

information to third parties in the three years preceding the request (including the purpose and dates of such use/provision)[139].

(109) Under the CIA, individuals also have a right to access their personal credit information (Article 38(1) CIA) and to obtain correction of inaccurate data (Article 38(2)-(3) CIA)[140]. Moreover, in addition to the general right to erasure under PIPA (see recital (77)), the CIA provides for a specific right to erasure of personal credit information that has been retained beyond the retention periods mentioned in recital (104), i.e. five years (for personal credit information that was necessary to establish or maintain a commercial relationship) or three months (for other types of personal credit information)[141]. A request for erasure may exceptionally be refused where further retention is necessary in the circumstances described in recital (105). If an individual requests erasure, but one of the exceptions applies, specific safeguards must be applied to the concerned credit information (Article 38-3(3) CIA and Article 33-3 CIA Enforcement Decree). For example, the information must be kept separately from other information, may only be accessed by an authorised person and must be subject to specific security measures.

(110) In addition to the rights mentioned in recital (109), the CIA guarantees individuals a right to request a controller to stop contacting them for direct marketing purposes (Article 37(2) of the Act) and a right to data portability. As regards the latter, the CIA allows individuals to request transmission of their personal credit information to themselves or to certain third parties (such as financial institutions and credit rating companies). The personal credit information must be processed and transmitted to the third party in a format that can be processed by an information-processing device (such as a computer).

(111) To the extent that the CIA contains specific rules compared to PIPA, the Commission therefore considers that also these rules ensure a level of protection essentially equivalent to that afforded under Regulation (EU) 2016/679.

2.4 Oversight and enforcement

(112) In order to ensure that an adequate level of data protection is guaranteed in practice, an independent supervisory authority tasked with powers to monitor and enforce compliance with the data protection rules should be in place. This authority should act with complete independence and impartiality in performing its duties and exercising its powers.

2.4.1 Independent oversight

---

139 Article 35 CIA. Certain commercial organisations, e.g. cooperatives and public corporations (Article 21(2) CIA Enforcement Decree) are subject to additional transparency requirements, e.g. to make certain information publicly available (Article 31 CIA) and to inform individuals of possible disadvantages to their credit rating score when they engage in financial transactions that pose credit risks (Article 35-2 CIA).

140 As regards the conditions and exceptions to the rights of access and correction, the rules of PIPA (described in recitals (76)-(77)) apply. In addition, further modalities are laid down in Article 38(4)-(8) CIA and Article 33 CIA Enforcement Decree. In particular, a commercial operator that has corrected or deleted inaccurate credit information must notify the individual thereof. In addition, any third party to which that information was disclosed within the previous six months must be notified, and the concerned individual must be informed thereof. If an individual is not satisfied with how a request for correction was handled, (s)he can lodge a request with the PIPC, which verifies the actions of the controller and may impose corrective measures.

141 Article 38-3 CIA.

(113) In the Republic of Korea, the independent authority in charge of monitoring and enforcing PIPA is the PIPC. The PIPC is composed of a Chairperson, a Vice Chairperson and seven Commissioners. The Chairperson and Vice Chairperson are appointed by the President upon recommendation of the Prime Minister. Of the Commissioners, two are appointed by the President upon recommendation of the Chairperson and five upon recommendation of the National Assembly (of which two upon recommendation from the political party to which the President belongs and three upon recommendation from other political parties (Article 7-2(2) PIPA), which helps to counteract partisanship in the appointment process)[142]. This procedure is in line with the requirements applicable to the appointment of members of data protection authorities in the Union (Article 53(1) of Regulation (EU) 2016/679). Moreover, all Commissioners must abstain from any profit-related business, political activities and from holding positions in public administration or the National Assembly (Articles 7-6 and 7-7(1) lit. 3 PIPA)[143]. All Commissioners are subject to specific rules preventing them from participation in deliberations in case of a possible conflict of interest (Article 7-11 PIPA). The PIPC is assisted by a Secretariat (Article 7-13) and may establish sub-commissions (consisting of three Commissioners) to handle minor violations and recurring matters (Article 7-12 PIPA).

(114) Each member of the PIPC is appointed for three years and may be reappointed once (Article 7-4(1) PIPA). Commissioners may only be dismissed under specific circumstances, namely if they are no longer able to perform their duties due to long-term mental or physical disability, act in violation of the law, or fulfil one of the grounds for disqualification from office[144] (Article 7-5 PIPA). This provides them with institutional protection in the exercise of their functions.

(115) More generally, Article 7(1) PIPA explicitly guarantees the PIPC's independence, and Article 7-5(2) PIPA requires Commissioners to perform their duties independently, according to law and their conscience[145]. The institutional and procedural safeguards described, including with respect to the appointment and dismissal of its members, ensure that the PIPC acts with complete independence, free from external influence or instructions. Moreover, as a central administrative agency, the PIPC annually proposes its own budget (which is reviewed by the Ministry of Finance as part of the overall national budget before adoption by the National Assembly) and is in charge of its own personnel management. The PIPC has a current budget of about 35 million euro and

142 Only individuals that meet the following criteria may be appointed as PIPC Commissioners: senior civil servants in charge of personal information affairs; former judges, public prosecutors or lawyers having practised for at least 10 years; former managers with experience in data protection that served in a public institution or organisation for more than three years, or that have been recommended by such institution or organisation; and former associate professors with professional knowledge in the field of data protection that served for at least five years in an academic institution (Article 7-2 PIPA).

143 See also Article 4-2 PIPA Enforcement Decree.

144 See Article 7-7 PIPA, according to which non-Korean nationals and members of political parties may not become members of the PIPC. The same applies to individuals that have received certain types of criminal sanctions, have been removed from office by disciplinary action within the last five years, etc. (Article 7-7 PIPA in conjunction with Article 33 of the Public Officials Act).

145 While Article 7(2) PIPA refers to the general power of the Prime Minister under Article 18 of the Government Organisation Act to suspend or revoke – with the approval of the President – any unlawful or unjust disposition of a central administrative agency, no such power is granted with respect to the PIPC's investigatory or enforcement powers (see Article 7(2) lit. 1, 2 PIPA). According to explanations received from the Korean government, Article 18 Government Organisation Act is intended to provide the Prime Minister with the possibility to act in extraordinary circumstances, e.g. to mediate a disagreement between different governmental agencies. However, the Prime Minister has never made use of this power since this provision was adopted in 1963.

has 154 staff members (including 40 employees specialised in information and communications technology, 32 employees focusing on investigations and 40 legal experts).

(116) The tasks and powers of the PIPC are mainly provided for in Articles 7-8 and 7-9, as well as in Articles 61-66 PIPA[146]. In particular, the tasks of the PIPC include advising on laws and regulations related to data protection, developing data protection policies and guidelines, investigating infringements of individual rights, handling complaints and mediating disputes, enforcing compliance with PIPA, ensuring education and promotion in the area of data protection, and exchanging and cooperating with third country data protection authorities[147].

(117) Based on Article 68 PIPA in conjunction with Article 62 of the PIPA Enforcement Decree, certain tasks of the PIPC have been delegated to the Korea Internet and Security Agency, namely: (1) education and public relations, (2) training of specialists and development of criteria for privacy impact assessments, (3) the handling of requests for designating a so-called privacy impact assessment institution, (4) the handling of requests for indirect access to personal data held by public authorities (Article 35(2) PIPA), and (5) the task of requesting materials and carrying out inspections with respect to complaints received through the so-called Privacy Call Centre. In the context of the handling of complaints through the Privacy Call Centre, the Korea Internet and Security Agency transmits the case to the PIPC or to the prosecution if it finds that a violation of the law has occurred. The possibility of submitting a complaint to the Privacy Call Centre does not prevent individuals from directly lodging a complaint with the PIPC or from turning to the PIPC if they consider that their complaint was not satisfactorily handled by the Korea Internet and Security Agency.

2.4.2 Enforcement, including sanctions

(118) With a view to ensuring compliance with PIPA, the legislator has granted the PIPC both investigatory and enforcement powers, ranging from recommendations to administrative fines. These powers are further complemented by a regime of criminal sanctions.

(119) As regards investigatory powers, if a violation of PIPA is suspected or has been reported, or where necessary for the protection of data subject rights against infringements, the PIPC may conduct on-site inspections and request all relevant materials (such as articles and documents) from personal data controllers (Article 63 PIPA in conjunction with Article 60 of the PIPA Enforcement Decree)[148].

(120) In terms of enforcement, under Article 61(2) PIPA, the PIPC may provide advice to data controllers on how to improve the level of personal data protection of specific processing activities. Data controllers must make good faith efforts to implement such advice and are required to inform the PIPC of the outcome. Moreover, when there are

---

146 When necessary to carry out the tasks pursuant to Article 7-9(1) PIPA, the PIPC may solicit the opinions of relevant public officials, experts in data protection, civic organisations and relevant business operators. In addition, the PIPC may request relevant materials, may issue recommendations for improvement and inspect whether these are implemented (Article 7-9(2)-(5) PIPA).

147 See also Article 9 PIPA (three-yearly Master Plan for the protection of personal information) Article 12 PIPA (Standard Personal Information Protection Guidelines), Article 13 PIPA (policies for the promotion and support of self-regulation)

148 The PIPC may furthermore enter the premises of the controller to inspect the status of business operations, records, documents, etc. (Article 63(2) PIPA). See also Article 45-3 CIA and Article 36-4 CIA Enforcement Decree with respect to the PIPC's powers under that Act.

reasonable grounds to believe that a violation of PIPA has occurred and failure to take action is likely to cause damage that is difficult to remedy, the PIPC may impose corrective measures (Article 64(1) PIPA)[149]. Section 5 of Notification 2021-5 (Annex I) clarifies, with binding effect, that these conditions are fulfilled with respect to the violation of any PIPA provision that protects the privacy rights of individuals with respect to personal information[150]. The measures that the PIPC is empowered to take include ordering cessation of the conduct causing the violation, temporary suspension of the data processing or any other necessary measures. Failure to comply with a corrective measure may lead to a sanction by means of a fine of a maximum amount of 50 million won (Article 75(2) lit. 13 PIPA).

(121) With respect to certain public authorities (such as the National Assembly, central administrative agencies, local government bodies and the courts), Article 64(4) PIPA provides that the PIPC may "recommend" any of the corrective measures mentioned in recital (120) and that these authorities are required to comply with such a recommendation unless there are extraordinary circumstances. According to Section 5 of Notification 2021-5, this refers to extraordinary factual or legal circumstances of which the PIPC was not aware when making its recommendation. The concerned public authority may only invoke such extraordinary circumstances if it clearly demonstrates that no infringement occurred and the PIPC determines that this is indeed not the case. Otherwise, the public authority has to follow the PIPC's recommendation and "take a corrective measure, including to immediately stop the action, and compensate for damages in the exceptional case where an illegal act was nevertheless committed."

(122) The PIPC may also request other administrative agencies with specific competence under sectoral legislation (e.g. health, education) to carry out an investigation – alone or jointly with the PIPC – into (suspected) privacy violations by controllers operating in these sectors under their jurisdiction, and to impose corrective measures (Article 63(4)-(5) PIPA). In that case, the PIPC determines the grounds, object and scope of the investigation[151]. In turn, the relevant administrative agency must submit an inspection plan to the PIPC and notify the PIPC of the result of the inspection. The PIPC can recommend a specific corrective measure to be taken, which the relevant agency must endeavour to implement. In any event, such a request does not limit the PIPC's competence to carry out its own investigation or impose sanctions.

(123) In addition to its corrective powers, the PIPC may impose administrative fines between 10 and 50 million won for infringements of various PIPA requirements (Article 75 PIPA)[152]. Among others, this includes non-compliance with the

149 See also Article 45-4 CIA with respect to the PIPC's powers under the CIA.

150 Section 5 of the Notification provides that "substantial ground to deem that there has been infringement with respect to personal information, and failure to take action is likely to cause damage that is difficult to remedy within the meaning of Paragraphs 1 and 2 of Article 64 PIPA, refers to a violation of any of the principles, rights and duties included in the law to protect individuals' rights to personal information." The same applies to the powers of the PIPC under Article 45-4 of the CIA.

151 Article 60 PIPA Enforcement Decree

152 Moreover, where personal information processing and protection systems operated by a controller have been certified as being in compliance with PIPA, but where the certification criteria pursuant to Article 34-2(1) of the PIPA Enforcement Decree have in fact not been satisfied, or in case of a serious infringement of any "[personal] information protection-related statute", the PIPC may revoke the certification (Article 32-2(3), (5) PIPA). The PIPC shall notify the controller of such revocation and shall publicly announce it, or publish it on its website or in the Official Gazette (Article 34-4 PIPA Enforcement Decree). Administrative fines (Article 52 CIA) and criminal sanctions (Article 50 CIA) are also foreseen for violations of the CIA.

requirements for the lawfulness of processing, failure to take the necessary security measures, failure to notify data subjects in case of a data breach, non-compliance with the requirements for sub-processing, failure to establish and disclose a privacy policy, failure to designate a privacy officer, or failure to act upon a request by the data subject in the exercise of his or her individual rights, as well as certain procedural violations (non-cooperation during an investigation). In case of breaches of several provisions of PIPA by the same controller, a fine may be imposed for each violation, and the number of individuals affected will be taken into account in setting the level of the fine.

(124) Moreover, where reasonable grounds exist to suspect a violation of PIPA or any other "data protection-related statutes", the PIPC may submit a criminal complaint to the competent investigative agency (such as a prosecutor, see Article 65(1) PIPA). In addition, the PIPC may advise the controller to take disciplinary action against the person responsible (including the manager in charge, see Article 65(2) PIPA). Upon receiving such advice, the controller must comply[153] with it and must notify the PIPC in writing of the result (Article 65 of PIPA in conjunction with Article 58 of the PIPA Enforcement Decree).

(125) As regards advice pursuant to Article 61, corrective measures pursuant to Article 64, accusation or advice for disciplinary action pursuant to Article 65 and the imposition of administrative fines pursuant to Article 75 PIPA, the PIPC may publicise the facts – i.e. the infringement, the entity having infringed the law and the imposed measure(s) – by posting them on its website or in a general, nationwide daily newspaper (Article 66 PIPA in conjunction with Article 61(1) of the PIPA Enforcement Decree)[154].

(126) Finally, compliance with the data protection requirements in PIPA (as well as other "data protection-related statutes") is supported by a regime of criminal sanctions. In this respect, Articles 70-73 PIPA contain penalty provisions that can lead to the imposition of either a fine (between 20 and 100 million won) or imprisonment (with the maximum sentence varying between 2 and 10 years). Relevant infringements include, among others, the use of personal data or provision of such data to a third party without the necessary consent, the processing of sensitive information contrary to the prohibition in Article 23(1) PIPA, non-compliance with applicable safety requirements resulting in the personal data being lost, stolen, divulged, forged, altered or damaged, failure to take the necessary measures to correct, erase or suspend personal data, or unlawful transfer of personal data to a third country[155]. According to Article 74 PIPA, in each of these cases the employee, agent or representative of the controller as well as the controller itself shall be liable[156].

---

153 According to Article 58(2) PIPA Enforcement Decree, in case special circumstances render compliance with the advice "impracticable", the controller has to provide a reasoned justification to the PIPC.

154 In deciding whether to make such a public disclosure, the PIPC shall take into account the substance and severity of the violation, its length and frequency, as well as its consequences (extent of damage). The concerned entity shall be given prior notice and the possibility to defend itself. See Article 61(2), (3) PIPA Enforcement Decree.

155 See Article 71 lit. 2 in conjunction with Article 18(1) PIPA (failure to respect the conditions in Article 17(3) PIPA, to which Article 18(1) refers). See also Article 75(2) lit. 1 in conjunction with Article 17(2) PIPA (failure to provide necessary information to the individual concerned pursuant to Article 17(2) PIPA, to which Article 17(3) refers).

156 Moreover, Article 74-2 PIPA allows for the confiscation of any money, goods or other profits acquired as a consequence of the violation, or, if confiscation is impossible, the "collection" of the benefit unlawfully obtained.

(127) In addition to the criminal sanctions provided in PIPA, the misuse of personal data may also constitute an offence under the Criminal Act. This is the case in particular with respect to the violation of the secrecy of letters, documents or electronic records (Article 316), the disclosure of information subject to professional secrecy (Article 317), fraud by use of computers (Article 347-2) as well as embezzlement and breach of trust (Article 355).

(128) The Korean system therefore combines different types of sanctions, from corrective measures and administrative fines to criminal sanctions, which are likely to have a particularly strong deterrent effect on controllers and the individuals handling the data. Immediately after its establishment in 2020, the PIPC started to make use of its powers. The PIPC's annual report 2021 shows that the PIPC already issued a number of recommendations, administrative fines and corrective orders, both against the public sector (around 34 public authorities) and private operators (around 140 companies)[157]. Notable cases include, for example, the imposition of a fine of 6.7 billion won in December 2020 on a company for violating different provisions of PIPA (including security requirements, requirements for consent for third party provision and transparency)[158] and a fine of 103.3 million won in April 2021 on an AI technology company (for violating, amongst other provisions, the rules on lawfulness of processing, in particular consent, and the processing of pseudonymised information)[159]. In August 2021, the PIPC finalised another investigation into the activities of three companies, which led to corrective measures and the imposition of fines of up to 6.47 billion won (inter alia, for failing to inform individuals about the disclosure of personal data to third parties, including transfers to third countries)[160]. Also, already before the recent reform, South Korea had a strong track record of enforcement, with the responsible authorities making use of the full range of enforcement actions, including administrative fines, corrective measures, and 'naming and sharing' with respect to a variety of controllers, including communication service providers (Korea Communications Commission), as well as commercial operators, financial institutions, public authorities, universities and hospitals (Ministry of Interior and Safety)[161]. On this basis, the Commission concludes that the Korean system ensures the effective enforcement of the data protection rules in practice, thereby guaranteeing a level of protection essentially equivalent to that under Regulation (EU) 2016/679.

2.5 Redress

[157] See the annual report of the PIPC 2021, pp. 50-55 (only available in Korean), at https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7511#LINK

[158] See at (only available in Korean) https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=6954#LINK.

[159] See at (only available in Korean) https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8.

[160] See at (only available in Korean): https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7497#LINK.

[161] See e.g. the annual report 2020 at (only available in Korean) https://www.pipc.go.kr/np/cop/bbs/selectBoardList.do?bbsId=BS079&mCode=D070020000 and the examples provided in English at https://www.privacy.go.kr/eng/enforcement_02.do.

(129) In order to ensure adequate protection and in particular the enforcement of individual rights, the data subject should be provided with effective administrative and judicial redress, including compensation for damages.

(130) The Korean system provides individuals with various mechanisms to effectively enforce their rights and obtain (judicial) redress.

(131) As a first step, individuals who consider that their data protection rights or interests have been violated can turn to the relevant controller. According to Article 30(1) lit. 5 PIPA, the controller's privacy policy shall among others include information on the rights of data subjects and how to exercise them. Moreover, it shall provide contact information – such as the name and telephone number of the privacy officer or the department responsible for data protection – to allow the filing of complaints ("grievances"). Within the organisation of the controller, the privacy officer is charged with handling complaints, the adoption of corrective measures in case of a privacy violation and remedial compensation (Article 31(2) lit. 3, (4) PIPA). The latter is relevant, for instance, in case of a data breach as the controller has to inform the data subject of the contact point(s) for reporting any damage, among others (Article 34(1) lit. 5 PIPA).

(132) In addition, PIPA offers several redress avenues to individuals against controllers. Firstly, any individual who considers that his or her data protection rights or interests have been violated by the controller may report such infringement directly to the PIPC and/or one of the specialised institutions designated by the PIPC to receive and handle complaints; this includes the Korea Internet and Security Agency, which for that purpose operates a personal information call centre (the so-called „Privacy Call Centre") (Article 62(1), (2) PIPA in conjunction with Article 59 of the PIPA Enforcement Decree). The Privacy Call Centre investigates and establishes infringements, provides counselling in relation to personal data processing (Article 62(3) PIPA) and may report infringements to the PIPC (but cannot take enforcement measures itself). The Privacy Call Centre receives a large numbers of complaints/requests (e.g. 177.457 in 2020, 159.255 in 2019 and 164.497 in 2018).[162] According to information received from the PIPC, the PIPC itself received around 1,000 complaints between August 2020 and August 2021. In response to a complaint, the PIPC may issue an advice for improvements, corrective measures, an "accusation" to the competent investigative agency (including a prosecutor) or advice for disciplinary action (see Articles 61, 64 and 65 PIPA). Decisions of the PIPC (such as a refusal to handle a complaint or a rejection on substance of a complaint) can be challenged under the Administrative Litigation Act[163].

(133) Second, according to Articles 40 to 50 PIPA in conjunction with Articles 48-14 to 57 of the PIPA Enforcement Decree, data subjects may bring claims to a so-called "Dispute Mediation Committee", which consist of representatives appointed by the Chairperson of the PIPC from members of the Senior Executive Service of the PICP and individuals appointed based on their experience in the area of data protection from among certain eligible groups (see Article 40(2), (3) and (7) PIPA, Article 48-14 of the

[162] See the annual report of the PIPC of 2021, p. 174. In 2020, such complaints concerned, for instance, the collection of data without consent, non-compliance with transparency obligations, violations of PIPA by processors, insufficient security measures, failure to respond to requests from data subjects, as well as general inquiries.

[163] In particular, individuals may appeal the exercise of, or refusal to exercise, public power by an administrative agency (Article 2(1) lit. 1, Article 3 lit. 1 Administrative Litigation Act). More detailed information on procedural aspects, including admissibility requirements, is provided in recital (181).

PIPA Enforcement Decree)[164]. The possibility to make use of mediation before the Dispute Mediation Committee provides an alternative avenue to obtain redress, but does not limit the right of the individual to instead turn to the PIPC or courts. In order to examine the case, the Committee may request the disputing parties to provide necessary materials and/or call for relevant witnesses to appear before it (Article 45 PIPA). Once the matter has been clarified, the Committee prepares a draft mediation award[165] on which a majority of its members must agree. Draft mediation may include suspension of the violation, necessary remedies (including restitution or compensation) as well as any measures necessary to prevent recurrence of the same or similar violation(s) (Article 47(1) PIPA). Where both parties agree to the mediation award, it will have the same effect as a settlement in court (Article 47(5) PIPA). Neither of the parties is prevented from initiating a court action while mediation is ongoing, in which case the latter will be suspended (see Article 48(2) PIPA)[166]. Annual figures issued by the PIPC show that individuals regularly make use of the procedure before the Dispute Mediation Committee, which often leads to a successful outcome. For example, in 2020, the Committee handled 126 cases, of which 89 were resolved before the Committee (with 77 cases where the parties already reached an agreement before the mediation process ended and 12 cases where the parties accepted the mediation proposal), leading to a 70.6% mediation rate.[167] Similarly, in 2019, the Committee handled 139 cases, of which 92 were resolved, leading to a 62.2% mediation rate.

(134) Moreover, where at least 50 individuals suffer damage, or their data protection rights have been violated in the same or similar manner following from the same (type of) incident[168], a data subject or a data protection organisation may apply for collective dispute mediation on behalf of such a collectivity; other data subjects may apply to join such mediation, which will be publicly announced by the Dispute Mediation Committee (Article 49(1) to (3) of PIPA in conjunction with Articles 52 to 54 of the PIPA Enforcement Decree)[169]. The Dispute Mediation Committee may select at least one person who most appropriately represents the common interest as a representative party (Article 49(4) PIPA). Where the controller rejects collective dispute mediation or does not accept the mediation award, certain organisations[170] may file a class-action lawsuit to address the violation (Articles 51 to 57 PIPA).

---

164 All of the members have a fixed term of office and may only be dismissed for just cause (see Articles 40(5), 41 PIPA). Moreover, Article 42 PIPA contains safeguards to protect against conflicts of interest.

165 See Article 44 PIPA. In addition, it may propose a draft settlement and recommend settlement without mediation (see Article 46 PIPA).

166 In addition, the Committee may reject mediation if it deems it inappropriate to mediate the dispute in view of its nature, or because the application for mediation was filed for an unfair purpose (Article 48 PIPA).

167 See the annual report of the PIPC of 2021, at p. 179-180. These cases concerned, inter alia, infringements of the requirement to obtain consent for the collection of data, the principle of purpose limitation, and data subject rights.

168 See Article 49(1) PIPA, according to which data subjects must suffer damage or an infringement of their rights "in an identical or similar manner", and Article 52 lit. 2 PIPA Enforcement Decree which makes it a requirement that "[m]ajor issues of the incident are common in fact or legally".

169 Moreover, even non-parties may benefit from a collective dispute mediation award accepted by the controller in that the Dispute Mediation Committee may advise the controller to prepare and submit a compensation plan that (also) covers them (Article 49(5) PIPA).

170 Namely, consumer groups or non-profit NGOs of a certain size in terms of membership whose stated purpose is data protection (albeit in case of the latter with the additional requirement that at least 100 data subjects that experienced the same (type of) infringement have submitted a request to file a class-action lawsuit). See Article 51 PIPA.

(135) Thirdly, in case of a privacy violation causing "damage" to the individual, the data subject has a right to appropriate redress in a "prompt and fair procedure" (Article 4 lit. 5 with Article 39 PIPA)[171]. The controller may exculpate itself by proving the absence of fault ("wrongful intent" or negligence). Where the data subject suffers damage as a result of loss, theft, divulgence, forgery, alteration or damage of/to his or her personal data, the Court may determine compensation of up to three times the actual damage, taking into account a number of factors (Article 39(3), (4) PIPA). Alternatively, the data subject may claim a "reasonable amount" of compensation not exceeding 3 million won (Article 39-2(1), (2) PIPA). Moreover, in accordance with the Civil Act, compensation may be claimed from any person "who causes losses to or inflicts injuries on another person by an unlawful act, intentionally or negligently"[172] or from a person "who has injured the person, liberty or fame of another or has inflicted any mental anguish to another person"[173]. Such tort liability following from the violation of data protection rules has been confirmed by the Supreme Court[174]. If damage has been caused by unlawful action of a public authority, a claim for compensation may furthermore be filed under the State Compensation Act[175]. A claim under the State Compensation Act may be filed with a specialised "Compensation Council", or directly with the Korean courts[176]. State liability also covers non-material damage (such as mental suffering)[177]. If the victim is a foreign national, the State Compensation Act applies as long as his or her country of origin equally ensures state compensation for Korean nationals[178].

(136) Fourthly, the Supreme Court has recognised that individuals have a right to claim injunctive relief for infringements of their rights under the Constitution, including the

---

171 Articles 43 to 43-3 CIA also lay down the liability to compensate for damages following from violations of that Act.

172 Article 750 Civil Act.

173 Article 751(1) Civil Act.

174 See, for example, Supreme Court Decision 2015Da251539, 251546, 251553, 251560, 251577, 30 May 2018. In addition, the Supreme Court confirmed that data breaches may lead to an award of damages under the Civil Act, see Supreme Court Decision 2011Da59834, 59858, 59841, 26 December 2012 (English summary available at http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm). In this case, the Supreme Court clarified that, to assess whether an individual suffered from emotional distress qualifying as compensable damage, several factors should be considered, such as the type and characteristics of the leaked information, the identifiability of the individual due to the breach, the possibility of access to the data by third parties, the extent to which the personal information was spread, whether this led to any additional infringements of individual rights, how the personal information was managed and protected, etc.

175 On the basis of the State Compensation Act, individuals may apply for compensation for damages inflicted by public officials in performing their official duties in violation of the law (Article 2(1) of the Act).

176 Articles 9 and 12 State Compensation Act. The Act establishes District Councils (chaired by the deputy prosecutor of the corresponding prosecutor's office), a Central Council (chaired by the Vice Minister of Justice) and a Special Council (in charge of compensation claims for damages inflicted by military personnel or civilian employees of the military, chaired by the Vice Minister of National Defense). Claims for compensation are in principle handled by District Councils, which under certain circumstances have to forward cases to the Central/Special Council, e.g. if the compensation exceeds a certain amount or in case an individual applies for re-deliberation. All Councils consist of members appointed by the Minister of Justice (e.g. from among public officials of the Ministry of Justice, judicial officers, lawyers, and persons having an expertise in relation to state compensation) and are subject to specific rules on conflict of interest (see Article 7 Enforcement Decree of the State Compensation Act).

177 See Article 8 State Compensation Act (which refers to the Civil Act), as well as Article 751 Civil Act.

178 Article 7 State Compensation Act.

right to the protection of personal data[179]. In this context, a court may for instance order controllers to suspend or stop any unlawful activity. In addition, data protection rights, including the rights protected by PIPA, can be enforced via civil actions. This horizontal application of the constitutional protection of privacy to relationships between private parties has been recognised by the Supreme Court[180].

(137) Finally, individuals may file a criminal complaint pursuant to the Criminal Procedure Act (Article 223) with a public prosecutor or judicial police officer[181].

(138) The Korean system therefore offers various avenues to obtain redress, from easily accessible, low cost options (for instance by contacting the Privacy Call Centre or through (collective) mediation) to administrative (before the PIPC) and judicial avenues, including with the possibility to obtain compensation for damages.

3. ACCESS AND USE OF PERSONAL DATA TRANSFERRED FROM THE EUROPEAN UNION BY PUBLIC AUTHORITIES IN THE REPUBLIC OF KOREA

(139) The Commission also assessed the limitations and safeguards, including the oversight and individual redress mechanisms available in Korean law as regards the collection and subsequent use by Korean public authorities of personal data transferred to controllers in Korea in the public interest, in particular for criminal law enforcement and national security purposes (government access). In this respect, the Korean government has provided the Commission with official representations, assurances and commitments signed at the highest ministerial and agency level that are contained in Annex II to this Decision.

(140) In assessing whether the conditions under which government access to data transferred to Korea under this Decision fulfil the "essential equivalence" test pursuant to Article 45(1) of Regulation (EU) 2016/679, as interpreted by the Court of Justice of the European Union in light of the Charter of Fundamental Rights, the Commission took into account in particular the following criteria.

(141) Firstly, any limitation to the right to the protection of personal data must be provided for by law and the legal basis which permits the interference with such a right must itself define the scope of the limitation on the exercise of the right concerned[182].

(142) Secondly, in order to satisfy the requirement of proportionality, according to which derogations from and limitations to the protection of personal data must apply only in so far as is strictly necessary in a democratic society to meet specific objectives of general interest equivalent to those recognized by the Union, the legislation of the third country in question which permits the interference must lay down clear and

---

179 Supreme Court Decision 93Da40614, 12 April 1996, and Decision 2008Da42430, 2 September 2011 (English summary available at https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord=).

180 See, for example, Supreme Court Decision 2008Da42430, 2 September 2011, (English summary available at https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord=).

181 As explained in recital (127), the misuse of data may constitute a criminal offense under the Criminal Act.

182 See *Schrems II*, paragraphs 174-175 and the case-law cited. See also, as regards access by public authorities of Member States, Case C-623/17 Privacy International, ECLI:EU:C:2020:790, paragraph 65; and Joined Cases C-511/18, C-512/18 and C-520/18 La Quadrature du Net and Others, ECLI:EU:C:2020:791, paragraph 175.

precise rules governing the scope and application of the measures in question and impose minimum safeguards so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse[183]. The legislation must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted[184] as well as subject the fulfilment of such requirements to independent oversight[185].

(143) Thirdly, that legislation and its requirements must be legally binding under domestic law. This concerns first of all the authorities of the third country in question, but these legal requirements must also be enforceable before courts against those authorities[186]. In particular, data subjects must have the possibility of bringing legal action before an independent and impartial tribunal in order to have access to their personal data, or to obtain the rectification or erasure of such data[187].

3.1 General legal framework

(144) The limitations and safeguards that apply to the collection and subsequent use of personal data by Korean public authorities follow from the overarching constitutional framework, specific laws that regulate their activities in the areas of criminal law enforcement and national security, as well as the rules that specifically apply to the processing of personal data.

(145) Firstly, access to personal data by Korean public authorities is governed by general principles of legality, necessity and proportionality that follow from the Korean Constitution[188]. In particular, fundamental rights and freedoms (including the right to privacy and the right to privacy of correspondence)[189] may only be restricted by law and when necessary for national security, or the maintenance of law and order for public welfare. Such restrictions may not affect the essence of the right or freedom at stake. With respect to searches and seizures specifically, the Constitution provides that they may only take place as provided by law, on the basis of a warrant issued by a judge and in respect of due process[190]. Finally, individuals can invoke their rights and freedoms before the Constitutional Court if they believe that they have been infringed by public authorities in the exercise of their powers[191]. Similarly, individuals that have

183 See Schrems II, paragraphs 176 and 181, as well as the case-law cited. See also, as regards access by public authorities of Member States, *Privacy International*, paragraph 68; and *La Quadrature du Net and Others*, paragraph 132.

184 See *Schrems II*, paragraph 176. See also, as regards access by public authorities of Member States, *Privacy International*, paragraph 68; and *La Quadrature du Net and Others*, paragraph 132.

185 See *Schrems II*, paragraph 179.

186 See *Schrems II*, paragraphs 181-182.

187 See *Schrems I*, paragraph 95 and *Schrems II*, paragraph 194. In that respect, the CJEU has notably stressed that compliance with Article 47 of the Charter of Fundamental Rights, guaranteeing the right to an effective remedy before an independent and impartial tribunal, "contributes to the required level of protection in the European Union [and] must be determined by the Commission before it adopts an adequacy decision pursuant to Article 45(1) of Regulation (EU) 2016/679" (*Schrems II*, paragraph 186).

188 See Annex II, section 1.1.

189 Article 37(2) of the Constitution.

190 Article 16 and 12(3) of the Constitution. Article 12(3) of the Constitution furthermore sets out the exceptional circumstances in which warrantless searches or seizures may take place (although an *ex post* warrant is still required), i.e. in flagrante delicto or, for crimes subject to imprisonment of at least three years, if there is a risk that evidence will be destroyed or the suspect will disappear.

191 Article 68(1) Constitutional Court Act.

suffered damages because of an unlawful act committed by a public official in the course of official duties have a right to claim just compensation[192].

(146) Secondly, as described in more detail in sections 3.2.1 and 3.3.1, the general principles mentioned in recital (145) are also reflected in the specific laws that regulate the powers of law enforcement and national security authorities. For example, with respect to criminal investigations, the Criminal Procedure Act (CPA) provides that compulsory measures may only be taken where explicitly provided for in the CPA and to the least extent necessary to achieve the purpose of the investigation[193]. Similarly, Article 3 of the Communications Privacy Protection Act (CPPA) prohibits access to private communications except on the basis of the law and subject to the limitations and safeguards set out therein. In the area of national security, the National Intelligence Service Act (NIS Act) provides that any access to communications or location information must comply with the law and subjects abuse of power and violations of the law to criminal sanctions[194].

(147) Thirdly, the processing of personal data by public authorities, including for law enforcement and national security purposes, is subject to data protection rules under PIPA[195]. As a general principle, Article 5(1) PIPA requires public authorities to develop policies to prevent "abuse and misuse of personal information, indiscrete surveillance and tracking, etc. and to enhance the dignity of human beings and individual privacy." In addition, any controller must process personal data in a manner which minimises the possibility of infringing upon the privacy of the data subject (Article 3(6) PIPA).

(148) All PIPA requirements, as described in detail in section 2, apply to the processing of personal data for law enforcement purposes. This includes the core principles (such as lawfulness and fairness, purpose limitation, accuracy, data minimisation, storage limitation, security and transparency), obligations (for instance with respect to data breach notification and sensitive data) and rights (to obtain access, correction, deletion and suspension).

(149) While the processing of personal data for national security purposes is subject to a more limited set of provisions under PIPA, the core principles, as well as the rules on oversight, enforcement and redress, apply[196]. More specifically, Articles 3 and 4 PIPA lay down the general data protection principles (lawfulness and fairness, purpose limitation, accuracy, data minimisation, security and transparency) and individual rights (the right to be informed, the right of access, and the rights to correction, deletion and suspension)[197]. Article 4(5) PIPA furthermore provides individuals with the right to appropriate redress for any damage arising out of the processing of their

---

192 Article 29(1) of the Constitution.

193 Article 199(1) CPA. More generally, when exercising their powers under the CPA, public authorities must respect the fundamental rights of criminal suspects and any other person concerned (Article 198(2) CPA).

194 Article 14 NIS Act.

195 See Annex II, section 1.2.

196 Article 58(1) lit. 2 PIPA. See also Section 6 of Notification No 2021-5 (Annex I). This exemption from certain provisions of PIPA only applies when personal data is processed "for national security purposes". Once the national security situation justifying the data processing has ended, the exemption can no longer be relied upon and all PIPA requirements apply.

197 Such rights may only be restricted when provided for by law to the extent and for as long as necessary and proportionate to protect an important objective of public interest, or where granting the right may cause damage to the life or body of a third party, or unjustified infringement of property and other interests of a third party. See Section 6 of Notification No 2021-5.

personal data in a prompt and fair procedure. This is complemented by more specific obligations to only process personal data to the minimum extent necessary to attain the intended purpose and for the minimum period, to put in place the necessary measures to ensure safe data management and appropriate processing (such as technical, managerial and physical safeguards), as well as to put in place measures for the appropriate handling of individual grievances (complaints)[198]. Finally, the general principles of legality, necessity and proportionality from the Korean Constitution (see recital (145)) also apply to the processing of personal data for national security purposes.

(150) These general limitations and safeguards can be invoked by individuals before independent oversight bodies (e.g. the PIPC and/or the National Human Rights Commission, see recitals (177) - (178)) and courts (see recitals (179) - (183)) to obtain redress.

3.2 Access and use by Korean public authorities for criminal law enforcement purposes

(151) The law of the Republic of Korea imposes a number of limitations on the access and use of personal data for criminal law enforcement purposes, and provides oversight and redress mechanisms which are in line with the requirements referred to in recitals (141) to (143) of this Decision. The conditions under which such access can take place and the safeguards applicable to the use of those powers are assessed in detail in the following sections.

3.2.1 Legal bases, limitations and safeguards

(152) Personal data processed by Korean controllers that would be transferred from the Union under this Decision[199] may be collected by Korean authorities for criminal law enforcement purposes in the context of a search or seizure (on the basis of the CPA), by accessing communication information (on the basis of the CPPA), or by obtaining subscriber data through requests for voluntary disclosure (on the basis of the Telecommunications Business Act, TBA)[200].

3.2.1.1 Searches and seizures

(153) The CPA provides that a search or seizure may only take place if a person is suspected of a crime, it is necessary for the investigation and a connection is established between

198 Article 58(4) PIPA.

199 See Annex II, section 2.1. The official representation of the Korean Government (Section 2.1 of Annex II) also refers to the possibility to collect financial transaction information for the purpose of preventing money laundering and terrorism financing on the basis of the Act on Reporting and Using Specified Financial Transaction Information (ARUSFTI). However, the ARUSFTI only imposes disclosure obligations on controllers that process personal credit information pursuant to the CIA and are subject to FSC oversight (see recital (13)). Since the processing of personal credit information by such controllers is excluded from the scope of this Decision, the ARUSFTI is not relevant for the present assessment.

200 Article 3 CPPA also mentions the Military Court Act as a possible legal basis for the collection of communications data. However, that Act governs the collection of information on military personnel and can only apply to civilians in a limited number of cases (e.g. if military personnel and civilians would commit a crime together, or if an individual commits a crime against the military, proceedings may be initiated before a military court, see Article 2 Military Court Act). In any event, it lays down general provisions governing searches and seizures that are similar to the CPA (see e.g. Articles 146-149 and 153-156 Military Court Act) and for example provide that postal mail may only be collected when necessary for an investigation and on the basis of a warrant from the Military Court. To the extent that electronic communications would be collected on the basis of this Act, the limitations and safeguards of the CPPA would apply. See Annex II, section 2.2.2 and footnote 50.

the investigation and the person to be searched or article to be inspected or seized[201]. Moreover, a search or seizure (as any compulsory measure) may only be authorised/carried out to the least extent necessary[202]. If a search concerns a computer disc or other data storage medium, in principle only the necessary data itself (copied or printed out) will be seized rather than the entire medium[203]. The latter may only be seized when it is considered substantially impossible to print out or copy the required data separately, or when it is considered substantially impracticable to otherwise accomplish the purpose of the search[204]. The CPA therefore lays down clear and precise rules on the scope and application of these measures, thereby ensuring that the interference with the rights of individuals in case of a search or seizure will be limited to what is necessary for a specific criminal investigation and proportionate to the pursued purpose.

(154) In terms of procedural safeguards, the CPA requires that a warrant is obtained from a court to carry out a search or seizure[205]. A warrantless search or seizure is only exceptionally allowed, namely in urgent circumstances[206], *in loco* at the moment of arrest or detention of a criminal suspect[207], or where an article is discarded or voluntarily produced by a criminal suspect or third person (as regards personal data, by the concerned individual him/herself)[208]. Illegal searches and seizures are subject to criminal sanctions[209] and any evidence that is obtained in violation of the CPA is considered inadmissible[210]. Finally, the concerned individuals must always be notified about a search or seizure (including a seizure of their data) without delay[211], which will in turn facilitate the exercise of the individual's substantive rights and the right to redress (see in particular the possibility to challenge the execution of a seizure warrant, see recital (180)).

3.2.1.2 Access to communication information

---

201 Article 215(1) and (2) CPA. See also Articles 106(1), 107 and 109 CPA, which provide that courts may conduct searches and seizures as long as the concerned articles or persons are considered to be connected to a specific case. See Annex II, section 2.2.1.2.

202 Article 199(1) CPA.

203 Article 106(3) CPA.

204 Article 106(3) CPA.

205 Article 215(1) and (2) CPA, Article 113 CPA. When applying for a warrant, the concerned authority must submit materials demonstrating the grounds for suspecting an individual of having committed a crime, that the search, inspection or seizure is necessary, and that the relevant articles to be seized exist (Article 108(1) Regulation on Criminal Procedure). The warrant itself must specify, inter alia, the names of the criminal suspect and the offence; the place, person or articles to be searched, or articles to be seized; the date of issuing; and the effective period of application (Article 114(1) in conjunction with Article 219 CPA). See Annex II, section 2.2.1.2.

206 That is, when it is impossible to obtain a warrant because of urgency at the scene of an offence (Article 216(3) CPA), in which case a warrant must still be obtained subsequently without delay (Article 216(3) CPA).

207 Article 216(1) and (2) CPA.

208 Article 218 CPA. Moreover, as explained in Section 2.2.1.2 of Annex II, voluntarily produced articles are only admitted as evidence in court proceedings if there is no reasonable doubt regarding the voluntary nature of the disclosure, which it is for the prosecutor to demonstrate.

209 Article 321 Criminal Act.

210 Article 308-2 CPA. In addition, an individual (and his/her counsel) may be present when a warrant for a search or seizure is being executed and may therefore also raise an objection at the time the warrant is being executed (Articles 121 and 219 CPA).

211 Article 121 and 122 CPA (with respect to searches), and Article 219 in conjunction with Article 106(4) CPA (with respect to seizures).

(155) On the basis of the CPPA, Korean criminal law enforcement authorities may take two types of measures[212]: on the one hand, the collection of "communication confirmation data"[213], which includes the date of telecommunications, their start- and end-time, the number of outgoing and incoming calls as well as the subscriber number of the other party, the frequency of use, log files on the use of telecommunication services and location information (for instance from transmission towers where signals are received); and, on the other hand, "communication-restricting measures", which cover both the collection of the content of traditional mail and the direct interception of the content of telecommunications[214].

(156) Communication confirmation data may only be accessed when necessary to conduct a criminal investigation or execute a sentence[215], on the basis of a warrant issued by a court[216]. In this respect, the CPPA requires that detailed information is provided both in the application for the warrant (e.g. on the reasons for the request, the relation with the target/subscriber and the necessary data) and in the warrant itself (e.g. on the objective, target and scope of the measure)[217]. Warrantless collection may only take place when grounds of urgency make it impossible to obtain court permission, in which case the warrant must be obtained and communicated to the telecommunication provider immediately after requesting the data[218]. If the court refuses to grant subsequent permission, the collected information must be destroyed[219].

(157) In terms of additional safeguards with respect to the collection of communication confirmation data, the CPPA imposes specific record-keeping and transparency requirements[220]. In particular, both criminal law enforcement authorities[221] and telecommunication providers[222] must keep records of requests and disclosures made. In addition, criminal law enforcement must in principle notify individuals of the fact

---

212 See also Annex II, section 2.2.2.1. Such measures may be taken with the compelled assistance of telecommunication operators upon providing such operators with a written permission obtained from a court (Article 9(2) CPPA), which must be kept by the operators (Article 15-2 CPPA and Article 12 CPPA Enforcement Decree). Telecommunication providers may refuse cooperation when information on the targeted individual as indicated in the court's written permission (for example the individual's telephone number) is incorrect, and are prohibited under all circumstances from disclosing passwords used for telecommunications (Article 9(4) CPPA).

213 Article 2(11) CPPA.

214 See Article 2(6) CPPA, which refers to "censorship" (opening mail without the consent of the party concerned or acquiring knowledge of, recording or withholding its contents through other means) and Article 2(7) CPPA, which refers to "wiretapping" (acquiring or recording the contents of telecommunications by listening to or communally reading the sounds, words, symbols or images of the communications through electronic and mechanical devices without the consent of the party concerned or interfering with their transmission and reception).

215 Article 13(1) CPPA. See also Annex II, section 2.2.2.3. In addition, real-time location tracking data and communication confirmation data concerning a specific base station may only be collected for the investigation of serious crimes or where it would otherwise be difficult to prevent the execution of a crime or collect evidence (Article 13(2) CPPA). This reflects the need to provide for additional safeguards in case of particularly privacy-intrusive measures, in line with the principle of proportionality.

216 Articles 13 and 6 CPPA.

217 See Article 13(3) and (9) in conjunction with Article 6(4) and (6) CPPA.

218 Article 13(2) CPPA.

219 Article 13(3) CPPA.

220 See Annex II, section 2.2.2.3.

221 Article 13(5) and (6) CPPA.

222 Article 13(7) CPPA. Moreover, telecommunication providers must report twice per year on the disclosure of communication confirmation data to the Ministry of Science and ICT.

that their communication confirmation data has been collected[223]. Such notification may only be deferred in exceptional circumstances, on the basis of an authorisation from the director of a competent district public prosecutors' office[224]. Such an authorisation may only be provided when notification is likely to (1) endanger national security, public security and order, (2) cause death or bodily injury, (3) impede fair judicial proceedings (for instance leading to the destruction of evidence or threatening of witnesses), or (4) defame the suspect, victims or other persons related to the case, or invade their privacy. In those cases, notification must be provided within 30 days once the ground(s) for deferral cease to exist[225]. Upon notification, individuals have a right to obtain information about the reasons for the collection of their data[226].

(158) Stricter rules apply with respect to communication-restricting measures, which may only be used when there is substantial reason to suspect that certain serious crimes specifically listed in the CPPA are being planned, are being committed, or have been committed[227]. Moreover, communication-restricting measures may only be taken as a measure of last resort and where it is difficult to otherwise prevent the commission of a crime, arrest a criminal, or collect evidence[228]. They must immediately be discontinued once they are no longer necessary, to ensure that the infringement of the privacy of communications is as limited as possible[229]. Information that has been illegally obtained by means of communication-restricting measures is not admitted as evidence in judicial or disciplinary proceedings[230].

(159) In terms of procedural safeguards, the CPPA requires that a court warrant is obtained in order to carry out communication-restricting measures[231]. Again, the CPPA requires that the application for a warrant and the warrant itself contain detailed information[232], including on the justification for the request, as well as the communications to be collected (which must be those of the suspect under investigation)[233]. Such measures may only be taken without a warrant in case of an imminent threat of organised crime

---

223 See Article 13-3(7) in conjunction with Article 9-2 CPPA. In particular, individuals must be notified within 30 days after a decision is taken (not) to prosecute or within 30 days following one year after a decision to suspend an indictment is taken (although notification must in any event be provided within 30 days following one year after the information has been collected), see Article 13-3(1) CPPA.

224 Article 13-3(2)-(3) CPPA.

225 Article 13-3(4) CPPA.

226 Article 13-3(5) CPPA. Upon request of the individual, a prosecutor or judicial police officer must provide the reasons in writing within 30 days after receiving the request, unless one of the exceptions for deferral of notification applies (Article 13-3(6) CPPA).

227 For example, insurrection, drug-related crimes, crimes involving explosives, as well as crimes related to national security, diplomatic relations, or military bases and installations, see Article 5(1) CPPA. See also Annex II, section 2.2.2.2.

228 Articles 3(2) and 5(1) CPPA.

229 Article 2 CPPA Enforcement Decree.

230 Article 4 CPPA.

231 Article 6(1), (2) and (5)-(6) CPPA.

232 An application for a warant must describe (1) the substantial reasons to (prima facie) suspect that one of the listed crimes is planned, being committed or has been committed as well as any supporting materials; (2) the communication-restricting measures as well as their target, scope, objective and effective period; and (3) the place where the measures would be executed and how they would be carried out (Article 6(4) CPPA and Article 4(1) CPPA Enforcement Decree). The warrant itself must specify the measures as well as their target, scope, effective period, place of execution and how they shall be carried out (Article 6(6) CPPA).

233 The target of a communication-restricting measure must be specific mail items or telecommunications sent or received by the suspect, or mail items or telecommunications sent or received by the suspect during a fixed period of time (Article 5(2) CPPA).

or where another serious crime that may directly cause death or serious injury is imminent, and an emergency exists that makes it impossible to go through the regular procedure[234]. However, in that case an application for a warrant must be filed immediately after the measure is taken[235]. Communication-restricting measures may only be carried out for a maximum period of two months[236] and may only be extended with court approval if the conditions for carrying out the measures continue to be met[237]. The extended period may not exceed a total of one year, or three years for certain particularly serious crimes (such as crimes related to insurrection, foreign aggression, national security)[238].

(160) As is the case for the collection of communication confirmation data, the CPPA requires telecommunication providers[239] and law enforcement authorities[240] to keep records of the execution of communication-restriction measures, and provides for notification of the concerned individual, which may exceptionally be deferred where necessary on important public interest grounds[241].

(161) Finally, non-compliance with several of the limitations and safeguards of the CPPA (including for instance the obligations for obtaining a warrant, record-keeping and notification of the individual), both with respect to the collection of communication confirmation data and the use of communication-restricting measures, are subject to criminal sanctions[242].

(162) The powers of criminal law enforcement authorities to collect communications data on the basis of the CPPA (both the content of communications and communication confirmation data) are therefore circumscribed by clear and precise rules, and are subject to a number of safeguards. These safeguards in particular guarantee oversight of the execution of such measures, both ex ante (through prior judicial approval) and ex post (through record-keeping and reporting requirements), and facilitate individuals' access to effective remedies (by ensuring that they are informed about the collection of their data).

3.2.1.3 Requests for voluntary disclosure of subscriber data

---

234 Article 8(1) CPPA. However, collection of information in emergency situations must always take place in accordance with an "emergency censorship/wiretapping statement" and the authority carrying out the collection must keep a register of any emergency measure (Article 8(4) CPPA).

235 The collection must be immediately discontinued if the law enforcement agency fails to obtain court permission within 36 hours (Article 8(2) CPPA), in which case, as explained in Section 2.2.2.2 of Annex II, the collected information will in principle be destroyed. The court must also be notified in case emergency measures have been completed in such a short time as to obviate the need for permission (e.g. if the suspect is arrested immediately after initiating the interception, see Article 8(5) CPPA). In that case, the court must be provided with information on the objective, target, scope, period, place of execution and method of collection as well as the grounds for not filing a request for court permission (Article 8(6)-(7) CPPA).

236 Article 6(7) CPPA. If the objective of the measures is achieved earlier within that period, the measures must be discontinued immediately.

237 Article 6(7)-(8) CPPA.

238 Article 6(8) CPPA.

239 Article 9(3) CPPA.

240 Article 18(1) CPPA Enforcement Decree.

241 In particular, the prosecutor must notify the individual within 30 days from issuing an indictment or a disposition not to indict or arrest (Article 9-2(1) CPPA). The notification may be deferred with the approval of the head of the district public prosecutors' office if it would likely seriously endanger national security or disrupt the public safety and order, or when it would likely result in material harm to the lives and bodies of others (Article 9-2(4)-(6) CPPA).

242 Articles 16 and 17 CPPA.

(163) In addition to relying on the compulsory measures described in recitals (153) - (162), Korean law enforcement authorities may ask telecommunication providers for "communications data" on a voluntary basis, in support of a criminal trial, investigation or the execution of a sentence (Article 83(3) TBA). This possibility only exists with respect to limited datasets, i.e. the name, resident registration number, address and phone number of users, the dates on which users subscribe or terminate their subscription as well as user identification codes (meaning codes used to identify the rightful user of computer systems or communication networks)[243]. Since only individuals that directly contract services from a Korean telecommunications provider are considered "users"[244], EU individuals whose data has been transferred to the Republic of Korea would normally not fall within this category[245].

(164) Different limitations apply to such voluntary disclosures, both to the exercise of powers by the law enforcement authority and the response of the telecommunication operator. As a general requirement, law enforcement authorities must act in accordance with the constitutional principles of necessity and proportionality (Articles 12(1) and 37(2) of the Constitution), including when they request information on a voluntary basis. In addition, they have to comply with PIPA, in particular by only collecting minimum personal data, to the extent necessary to achieve a legitimate purpose, in a manner to minimise the impact on the privacy of individuals (such as Article 3(1), (6) PIPA). More specifically, requests to obtain communications data on the basis of the TBA must be made in writing and state the reasons for the request, the link to the relevant user and the scope of the requested data[246].

(165) Telecommunication providers are not required to comply with such requests and may only do so in accordance with PIPA. This means, in particular, that they must balance the different interests at stake and may not provide the data if doing so would likely infringe unfairly on the interests of the individual or a third party[247]. This would for example be the case if it is clear that the requesting authority abused its authority[248]. Telecommunication operators must keep records of disclosures under the TBA and report twice per year to the Minister of Science and ICT[249].

(166) In addition, in accordance with Section 3 of Notification No 2021-5 (Annex I), telecommunication providers in principle have to notify the concerned individual when they voluntarily comply with a request[250]. This will in turn enable the individual to exercise his/her rights and, in case his/her data is disclosed unlawfully, obtain redress, either against the controller (for instance for disclosing the data in violation of PIPA or for responding to a request that was clearly disproportionate) or against the law enforcement authority (for instance for acting beyond the limits of what is

243 Article 83(3) TBA. See also Annex II, section 2.2.3.

244 Article 2(9) TBA.

245 See also Annex II, section 2.2.3.

246 Article 83(4) TBA. Where it is impossible to provide a written request due to urgency, the written request must be provided as soon as the reason for the urgency disappears (Article 83(4) TBA).

247 Article 18(2) PIPA.

248 Supreme Court Decision No. 2012Da105482, 10 March 2016. See also Annex II, section 2.2.3, on this Supreme Court Decision.

249 Article 83(5)-(6) TBA.

250 This requirement is subject to limited and qualified exceptions, in particular if and for as long as the notification would jeopardise an ongoing criminal investigation or is likely to harm the life or body of another person, where those rights or interests are manifestly superior to the rights of the data subject. See Section 3, (iii) (1) of the Notification.

necessary and proportionate or for not respecting the procedural requirements of the TBA).

3.2.2 Further use of the information collected

(167) The processing of personal data collected by Korean criminal law enforcement authorities is subject to all requirements of PIPA, including with respect to purpose limitation (Article 3(1)-(2) PIPA), lawfulness of use and provision to third parties (Articles 15, 17 and 18 PIPA), international transfers (Articles 17 and 18 PIPA, in conjunction with Section 2 of Notification 2021-5)[251], proportionality/data minimisation (Article 3(1),(6) PIPA) and storage limitation (Article 21 PIPA)[252].

(168) With respect to the content of communications acquired through the execution of communication-restricting measures, the CPPA specifically limits the possible use thereof to the investigation, prosecution or prevention of serious crimes[253]; disciplinary proceedings for the same crimes; claims for damages raised by a party to the communications or where this is specifically allowed by other laws[254]. Moreover, collected content of telecommunications transmitted over the internet may only be retained with the approval from the court that authorised the communication-restricting measures[255], with a view of using it for the investigation, prosecution or prevention of serious crimes[256]. More generally, the CPPA prohibits the disclosure of confidential information obtained from communication-restricting measures, and the use of such information to damage the reputation of those that were subject to the measures[257].

3.2.3 Oversight

(169) In Korea, the activities of criminal law enforcement authorities are supervised by different bodies[258].

(170) Firstly, the police is subject to internal oversight by an Inspector-General[259], which carries out legality control, including with respect to possible human rights violations. The Inspector-General was established to implement the Act on Public Sector Audits, which encourages the creation of self-auditing bodies and lays down specific requirements for their composition and tasks. In particular, the Act requires that the head of a self-auditing body is appointed from outside the relevant authority (such as

---

251 In particular, Korean public authorities are required to ensure, through a legally binding instrument, a level of protection equivalent to PIPA, see also recital (90).

252 See also Annex II, section 1.2.

253 See recital (158).

254 Article 12 CPPA. See Annex II, section 2.2.2.2.

255 The prosecutor or police officer executing the communication-restricting measures must select the telecommunications to be retained within 14 days after the measures end and request court approval (in the case of a police offer, the application must be made to a prosecutor, who in turn submits the request to the court), see Article 12-2(1) and (2) CPPA.

256 An application for such an authorisation must contain information on the communication-restricting measures, a summary of the results of the measures, the reasons for retention (together with supporting materials) and the telecommunications to be retained (Article 12-2(3) CPPA). If no application is made, the acquired data must be deleted within 14 days after the end of the communication-restricting measure (Article 12-2(5) CPPA), and if the application is rejected, within seven days (Article 12-2(5) CPPA). In both cases, a report on the deletion must be filed to the court that authorised the collection within seven days.

257 Article 11(2) CPPA Enforcement Decree.

258 See Annex II, section 2.3.

259 See Annex II, section 2.3.1. See also https://www.police.go.kr/eng/knpa/org/org01.jsp.

former judges, professors) for a period of two to five years[260], can only be dismissed for justified reasons (for instance when unable to perform duties due to health reasons, or when subject to disciplinary action)[261] and is guaranteed independence to the largest extent possible[262]. The obstruction of a self-audit is subject to administrative fines[263]. Audit reports (which may include recommendations, requests for disciplinary action, and requests for compensation or correction) are communicated to the head of the relevant public authority, the Board of Audit and Inspection (BAI)[264] and, generally, made public[265]. The results of the implementation of the report must also be notified to the BAI[266] (see recital (173) on the oversight role and powers of the BAI).

(171) Secondly, the PIPC oversees compliance of data processing by criminal law enforcement authorities with PIPA and other laws that protect the privacy of individuals, including the laws that regulate the collection of (electronic) evidence for criminal law enforcement purposes, as described in section 3.2.1[267]. In particular, as the oversight of the PIPC extends to the lawfulness and fairness of data collection and processing (Article 3(1) PIPA), which will be infringed if personal data is accessed and used in violation of those laws[268], the PIPC can also investigate and enforce compliance with the limitations and safeguards described in section 3.2.1[269]. In exercising this oversight role, the PIPC can make use of all of its investigatory and remedial powers, as described in detail in section 2.4.2. Already before the recent reform of PIPA (i.e. in its previous supervisory role for the public sector), the PIPC carried out several oversight activities into the processing of personal data by criminal law enforcement authorities, e.g. in the context of the interrogation of suspects (Case No. 2013-16, 26 August 2013), with respect to the provision of notices to individuals about the imposition of administrative fines (Case No. 2015-02-04, 26 January 2015), the sharing of data with other authorities (Case No. 2018-15-146, 9 July 2018, Case No. 2018-25-308, 10 December 2018; Case No. 2019-02-015, 29 January 2019), the collection of fingerprints or photographs (Case No. 2019-17-273, 9 September 2019), the use of drones (Case No. 2020-01-004, 13 January 2020). In those cases, the PIPC investigated compliance with several provisions of PIPA (e.g. lawfulness of processing, the principles of purpose limitation and data minimisation) but also relevant provisions of other laws such as the Criminal Procedure Act, and, where necessary issued recommendations to bring the processing in line with data protection requirements.

(172) Thirdly, independent oversight is provided by the National Human Rights Commission (NHRC)[270], which can investigate violations of the rights to privacy and privacy of correspondence as part of its general mandate to protect the fundamental rights of Articles 10-22 of the Constitution. The NHRC is comprised of 11

260 Similarly, auditors are appointed on the basis of specific conditions laid down in the Act, see Articles 16 et seq. Act on Public Sector Audits.
261 Articles 8-11 Act on Public Sector Audits.
262 Article 7 Act on Public Sector Audits.
263 Article 41 Act on Public Sector Audits.
264 Article 23(1) Act on Public Sector Audits.
265 Article 26 Act on Public Sector Audits.
266 Article 23(3) Act on Public Sector Audits.
267 See Article 7-8(3), (4) and Article 7-9(5) PIPA.
268 See PIPC Notification No. 2021-5, section 6 (Annex I).
269 See also Annex II, section 2.3.4.
270 Article 1 Human Rights Commission Act (NHRC Act).

Commissioners that have to meet specific qualifications[271] and are appointed by the President in accordance with procedures laid down by law. In particular, four commissioners are appointed upon nomination by the National Assembly, four upon nomination by the President and three upon nomination by the Chief Justice of the Supreme Court[272]. The Chairperson is appointed by the President from among the Commissioners and must be confirmed by the National Assembly[273]. Commissioners (including the Chairperson) are appointed for a renewable term of three years and may only be dismissed when they are sentenced to imprisonment or are no longer capable of performing their duties due to prolonged physical or mental weakness (in which case two thirds of the Commissioners must agree to the dismissal)[274]. As part of an investigation, the NHRC may request the submission of relevant materials, conduct inspections and summon individuals to testify[275]. In terms of remedial powers, the NHRC may issue (public) recommendations to improve or correct specific policies and practices, to which public authorities must respond with a proposed implementation plan[276]. If the concerned authority fails to implement recommendations, it must inform the Commission thereof[277], which may in turn disclose such failure to the National Assembly, and/or make it public. According to the official representation from the Korean government (section 2.3.5 of Annex II), Korean authorities generally comply with NHRC recommendations and have a strong incentive to do so as their implementation has been assessed as part of a general, continuous evaluation under the authority of the Prime Minister's Office. Annual figures on its activities show that the NHRC is actively overseeing the activities of criminal law enforcement authorities, either on the basis of individual petitions or by means of ex officio investigations[278].

(173) Fourthly, general oversight of the legality of activities of public authorities is carried out by the BAI, which examines the revenue and expenditure of the State, but also, more generally, oversees compliance with the duties of public authorities with a view

---

271 To be appointed, a Commissioner must (1) have served for at least ten years at a university or an authorized research institute, at least as an associate professor; (2) have served as a judge, prosecutor, or attorney-at-law for at least ten years; (3) have been engaged in human rights activities for at least ten years (e.g. for a non-profit, non-governmental organisation or international organisation); or (4) have been recommended by civil society groups (Article 5(3) NHRC Act). Moreover, once appointed, the Commissioners are prohibited from holding a concurrent office in the National Assembly, local councils, or any State or local government (as a public official), see Article 10 NHRC Act.

272 Article 5(1) and (2) NHRC Act.

273 Article 5(5) NHRC Act.

274 Article 7(1) and Article 8 NHRC Act.

275 Article 36 NHRC Act. In accordance with Article 6(7) of the Act, the submission of materials or articles may be rejected if it would prejudice state confidentiality liable to have a substantial effect on state security or diplomatic relations or would present a serious obstacle to a criminal investigation or pending trial. In such cases, the Commission may request further information from the head of the relevant agency (which has to comply in good faith) where necessary to allow review whether the refusal to provide the information is justified.

276 Article 25(1), (3) NHRC Act.

277 Article 25(4) NHRC Act.

278 For example, between 2015 and 2019 the NHRC received between 1380 and 1699 petitions against criminal law enforcement authorities annually and dealt with any equally high number (e.g., it handled 1546 complaints against the police in 2018 and 1249 in 2019); it also conducted several ex officio investigations, as described in more detail in the NHRC's annual report 2018 (available at https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7602641) and the annual report 2019 (available at https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

to improving the operation of public administration[279]. The BAI is formally established under the President of the Republic of Korea, but retains an independent status with respect to its duties[280]. In addition, it is granted full independence with respect to the appointment, dismissal and organisation of its staff, and the compilation of its budget[281]. The BAI consists of a Chairperson (appointed by the President, with the consent of the National Assembly)[282] and six commissioners (appointed by the President upon recommendation of the Chairperson)[283], which must meet specific qualifications laid down by law[284] and may only be dismissed in case of impeachment, sentencing to imprisonment or inability to perform their duties due to long-term mental or physical weakness[285]. The BAI conducts a general audit on an annual basis, but may also conduct specific audits on matters of special interest. In carrying out an audit or inspection, the BAI may request the submission of documents and request the attendance of individuals[286]. The BAI may issue recommendations, request disciplinary actions, or file a criminal complaint[287].

(174) Finally, the National Assembly carries out parliamentary oversight of public authorities through investigations and inspections[288] of their activities[289]. It may request the disclosure of documents, compel the appearance of witnesses[290], recommend corrective measures (if it concludes that unlawful or improper activities have taken place)[291] and make the results of its findings public[292]. Where the National Assembly requests that corrective measures are taken – which may, for instance, include awarding compensation, taking disciplinary action or improving internal procedures – the concerned public authority is required to act without delay and report on the outcome to the National Assembly[293].

3.2.4 Redress

(175) The Korean system offers different (judicial) avenues to obtain redress, including compensation for damages.

---

279 Articles 20 and 24 of the Act on the Board of Audit and Inspection (BAI Act). See Annex II, 2.3.2.

280 Article 2(1) BAI Act.

281 Article 2(2) BAI Act.

282 Article 4(1) BAI Act.

283 Articles 5(1) and 6 BAI Act

284 For example, having served as a judge, public prosecutor or attorney-at-law for at least ten years, worked as a public servant, or professor or higher-ranking position at a university for at least eight years, or worked for at least ten years in a stock-listed corporation or government-invested institution (of which at least five years as an executive officer), see Article 7 BAI Act. In addition, Commissioners are prohibited from participating in political activities, and from concurrently holding offices in the National Assembly, administrative agencies, organisations subject to audit and inspection by the BAI or any other office or position that is remunerated (Article 9 BAI Ac).

285 Article 8 BAI Act.

286 See e.g. Article 27 BAI Act.

287 Articles 24 and 31-35 BAI Act.

288 Article 128 National Assembly Act and Articles 2, 3 and 15 Act on the Inspection and Investigation of State Administration. This includes annual inspections of government affairs as a whole but also investigations of specific matters.

289 See Annex, section 2.2.3.

290 Article 10(1) Act on the Inspection and Investigation of State Administration. See also Articles 128 and 129 National Assembly Act.

291 Article 16(2) Act on the Inspection and Investigation of State Administration.

292 Article 12-2 Act on the Inspection and Investigation of State Administration.

293 Article 16(3) Act on the Inspection and Investigation of State Administration.

(176) Firstly, PIPA provides individuals with a right of access, correction, deletion and suspension with respect to the personal data processed for criminal law enforcement purposes[294].

(177) Secondly, individuals can make use of the different redress mechanisms offered by PIPA if their data has been processed by a criminal law enforcement authority in violation of PIPA or in violation of the limitations and safeguards governing the collection of personal data in other laws (i.e. the CPA or CPPA, see recital (171)). In particular, individuals may lodge a complaint with the PIPC (including through the Privacy Call Centre operated by the Korea Internet and Security Agency[295]) or the Personal Information Dispute Mediation Committee[296]. These redress possibilities are not subject to further admissibility requirements. On the basis of the Administrative Litigation Act, individuals may furthermore appeal/challenge the decisions or inaction of the PIPC (see recital (132)).

(178) Thirdly, any individual[297] may lodge a complaint before the NHRC concerning a violation of the right to privacy and data protection by a Korean criminal law enforcement authority. The NHRC may recommend the rectification or improvement of any relevant statute, institution, policy or practice[298], or the implementation of remedies such as mediation[299], cessation of the human rights violation, compensation for damages and measures to prevent recurrence of the same or similar violations[300]. According to the official representation from the Korean government (section 2.4.2 of Annex II), this may also include the deletion of unlawfully collected personal data. While the NHRC does not have the power to issue binding decisions, it offers a more informal, low cost and easily accessible redress avenue, in particular because, as explained in Annex II, section 2.4.2, it does not require demonstrating an injury in fact for a complaint to be investigated[301]. This ensures that complaints of individuals concerning the collection of their data can be investigated, even if an individual is not in a position to demonstrate that his/her data was in fact collected (e.g. because notification of the individual has not yet taken place). The NHRC's annual activity reports show that individuals are also making use of this avenue in practice to

---

294 This right may be exercised directly vis-à-vis the competent authority, or indirectly via the PIPC (Article 35(2) PIPA). As described in more detail in recitals (76)-(78), exceptions to these rights will only apply when necessary to protect important (public) interests.

295 Article 62 PIPA.

296 Articles 40-50 PIPA and Articles 48-2 to 57 PIPA Enforcement Decree. See also Annex II, section 2.4.1.

297 As explained in Annex II, Section 2.4.2, although Article 4 NHRC Act refers to citizens and foreigners residing in the Republic of Korea, the term "residing" reflects a concept of jurisdiction rather than territory. Therefore, if the fundamental rights of a foreigner outside of Korea are violated by national institutions within Korea, that individual may file a complaint with the NHRC. This would be the case if personal data of a foreigner transferred to Korea is unlawfully accessed by Korean public authorities. See in particular the explanations provided at https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2.

298 Article 44 NHRC Act.

299 An individual may also request to resolve the complaint through mediation, see Articles 42 et seq. NRHC Act.

300 Article 42(4) NHRC Act. Moreover, the NHRC may adopt urgent relief measures in case of an ongoing infringement that is likely to cause damage difficult to remedy if left unattended, see Article 48 NHRC Act.

301 A complaint must in principle be filed within one year from the violation, but the NHRC may still decide to investigate a complaint that is lodged after that time period as long as the statute of limitation under criminal or civil law has not expired (Article 32(1) lit. 4 NHRC Act).

challenge activities of criminal law enforcement authorities, including with respect to the handling of personal data[302]. If an individual is not satisfied with the outcome of a procedure before the NHRC, it may challenge the NHRC's decisions (such as a decision not to continue the investigation of a complaint[303]) and recommendations before the Korean courts under the Administrative Litigation Act (see recital (181))[304]. Moreover, a procedure before the NHRC can further facilitate access to courts, as an individual could seek further redress against the public authority that unlawfully processed his/her data on the basis of the findings of the NHRC, in accordance with the procedures described in recitals (181)-(183).

(179) Finally, different judicial remedies are available, allowing individuals to invoke the limitations and safeguards described in section 3.2.1 to obtain redress[305].

(180) With respect to seizures (including of data), the CPA provides for the possibility to object to or challenge the execution of a warrant through a "quasi-complaint", by petitioning the competent court with a request to cancel or alter a disposition made by a prosecutor or police officer[306].

(181) More generally, individuals may challenge the actions[307] or omissions[308] of public authorities (including criminal law enforcement authorities) under the Administrative Litigation Act[309]. Administrative action is considered a 'challengeable disposition' if it directly impacts on civil rights and duties[310], which, as confirmed by the Korean

---

302 For example, the NHRC has in the past handled complaints and issued recommendations with respect to unlawful seizures and a violation of the requirement to inform individuals of a seizure (see pp. 80 and 91 of the NHRC's annual report 2018, available at https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746), as well as the unlawful processing of personal information by the police, prosecution and courts (see pp. 157-158 of the NHRC's annual report 2019, available at https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7603308, and p. 76 of the annual report 2019, available at https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

303 For example, if the NHRC is exceptionally not able to inspect certain materials or facilities because they concern state secrets liable to have a substantial effect on state security or diplomatic relations, or where the inspection would present a serious obstacle to a criminal investigation or pending trial, and where this prevents the NHRC from carrying out the investigation necessary to assess the merits of the petition received, it will inform the individual of the reasons why the complaint was rejected, in accordance with Article 39 NHRC Act. In this case, the individual could challenge the NHRC's decision under the Administrative Litigation Act.

304 See e.g. Seoul High Court Decision 2007Nu27259, 18 April 2008, confirmed by Supreme Court Decision 2008Du7854, 9 October 2008; Seoul High Court Decision 2017Nu69382, 2 February 2018.

305 See Annex II, 2.4.3.

306 Article 417 CPA in conjunction with Article 414(2) CPA. See also Supreme Court Decision No. 97Mo66, 29 September 1997.

307 The Administrative Litigation Act refers to a "disposition", i.e. the exercise of, or refusal to exercise, public power in a specific case.

308 Under the Administrative Litigation Act, this refers to the prolonged failure of an administrative agency to take a certain disposition contrary to a legal obligation to do so.

309 An administrative challenge may first be brought before administrative appeals commissions established under certain public authorities (e.g. the NIS, the NHRC) or before the Central Administrative Appeals Commission established under the Anti-Corruption and Civil Rights Commission (Article 6 Administrative Appeals Act and Article 18(1) Administrative Litigation Act), as a more informal redress avenue. However, a claim may also be brought directly before the Korean courts on the basis of the Administrative Litigation Act.

310 Supreme Court Decision 98Du18435, 22 October 1999, Supreme Court Decision 99Du1113, 8 September 2000, and Supreme Court Decision 2010Du3541, 27 September 2012.

government (section 2.4.3 of Annex II), is the case for measures to collect personal data, be it directly (for instance by intercepting communications), by way of binding disclosure requests (for instance to a service provider) or requests for voluntary cooperation. For a complaint under the Administrative Litigation Act to be admissible, an individual must have a legal interest in pursuing the claim[311]. According to case law of the Supreme Court, "legal interest" is interpreted as a "legally protected interest", i.e. a direct and specific interest protected by laws and regulations on which administrative dispositions are based (meaning not general, indirect and abstract interests of the public)[312]. Individuals have such a legal interest in case of any violation of the limitations and safeguards that apply to the collection of their personal data for criminal law enforcement purposes (under specific laws or PIPA). On the basis of the Administrative Litigation Act, a court may decide to revoke or alter an illegal disposition, issue a finding of nullity (i.e. a finding that the disposition does not have legal effect or its non-existence in the legal order) or issue a finding that an omission is illegal[313]. A final judgment under the Administrative Litigation Act is binding on the parties[314].

(182) In addition to challenging government action via administrative litigation, individuals may also file a constitutional complaint with the Constitutional Court regarding any infringement of their fundamental rights due to the exercise or non-exercise of governmental power (excluding judgments of the courts)[315]. If other remedies are available, these must be exhausted first. According to the case law of the Constitutional Court, foreign nationals may file a constitutional complaint to the extent their basic rights are recognised under the Korean Constitution (see the explanations in section 1.1)[316]. The Constitutional Court may invalidate the exercise of governmental power that caused the infringement or confirm that a certain failure to act is unconstitutional[317]. In that case, the relevant authority is required to take measures to comply with the decision of the Court.

---

311 Articles 12, 35 and 36 Administrative Litigation Act. In addition, a request for revocation/alteration of a disposition and a request to affirm the illegality of an omission must be filed within 90 days from the date the individual becomes aware of the disposition/omission and in principle no later than one year from the date the disposition is issued, or the omission occurred, unless there are justifiable reasons (Articles 20 and 38(2) Administrative Litigation Act). The notion of "justifiable reasons" has been interpreted broadly by the Supreme Court and requires assessing whether it is socially acceptable to allow bringing a belated complaint, in light of all the circumstances of the case (Supreme Court Decision 90Nu6521, 28 June 1991). As confirmed by the Korean government in section 2.4.3 of Annex II, this includes (but is not limited to) reasons for delay for which the concerned party cannot be held responsible (i.e. situations that are outside the control of the complainant, for instance where (s)he has not been notified of the collection of his/her personal information) or force majeure (e.g. a natural disaster, war).

312 Supreme Court Decision No. 2006Du330, 26 March 2006.

313 Articles 2 and 4 Administrative Litigation Act.

314 Article 30(1) Administrative Litigation Act.

315 Article 68(1) Constitutional Court Act. Constitutional complaints must be filed within 90 days after the individual has become aware of the infringement, and within one year after its occurrence. As also explained in Annex II, section 2.4.3., given that the procedure of the Administrative Litigation Act is applied to litigation under the Constitutional Court Act pursuant to Article 40 of the Constitutional Court Act, a complaint will still be admissible if there are "justifiable reasons", as interpreted in accordance with the Supreme Court case law described in footnote 312. If other remedies need to be exhausted first, a constitutional complaint must be filed within 30 days after the final decision on such a remedy (Article 69 Constitutional Court Act).

316 Constitutional Court Decision No. 99HeonMa194, 29 November 2001.

317 Article 75(3) Constitutional Court Act.

(183) Moreover, individuals may obtain compensation for damages before the Korean courts. This first of all includes the possibility to claim compensation for violations of PIPA committed by criminal law enforcement authorities, in accordance with Article 39 (see also recital (135)). More generally, individuals may apply for compensation for damages inflicted by public officials in performing their official duties in violation of the law, on the basis of the State Compensation Act (see also recital (135))[318].

(184) The mechanisms described in recitals (176) - (183) provide data subjects with effective administrative and judicial remedies, enabling them in particular to enforce their rights, including the right to have access to their personal data, or to obtain the rectification or erasure of such data.

3.3 Access and use by Korean public authorities for national security purposes

(185) The law of the Republic of Korea contains a number of limitations and safeguards with respect to the access and use of personal data for national security purposes, and provides oversight and redress mechanisms which are in line with the requirements referred to in recitals (141) to (143) of this Decision. The conditions under which such access can take place and the safeguards applicable to the use of these powers are assessed in detail in the following sections.

3.3.1 Legal bases, limitations and safeguards

(186) In the Republic of Korea, personal data may be accessed for national security purposes on the basis of the CPPA, the TBA and the Act on Anti-Terrorism for the Protection of Citizens and Public Security (Anti-Terrorism Act)[319]. The main authority[320] with competences in the area of national security is the National Intelligence Service (NIS)[321]. The collection and use of personal data by the NIS must comply with relevant legal requirements (including PIPA and the CPPA)[322] and general guidelines prepared by the President and reviewed by the National Assembly[323]. As a general principle, the NIS must maintain political neutrality and protect the freedom and rights of individuals[324]. In addition, NIS staff must not abuse their official authority to force

318 Article 2(1) State Compensation Act.

319 See Annex II, section 3.1.

320 Exceptionally, the police and prosecution may also collect personal information for national security purposes (see footnote 327 and Annex II, section 3.2.1.2). In addition, the Korean military intelligence agency (the Defense Security Support Command, which is established under the Ministry of Defence), has powers in the area of national security. However, as explained in Annex II, section 3.1, it is only responsible for military intelligence and only carries out surveillance of civilians where this is necessary to conduct its military functions. In particular, it can only investigate military personnel, civilian employees of the military, persons in military training, persons in military reserve or recruit service and prisoners of war (Article 1 Military Court Act). When collecting communication information for national security purposes, the Defense Security Support Command is subject to the limitations and safeguards laid down by the CPPA and its Enforcement Decree.

321 The NIS' mandate is to collect, compile and distribute information on foreign countries (i.e. general information on trends and developments in relation to foreign countries, or the activities of state actors); intelligence related to countering espionage (including military and industrial espionage), terrorism and the activities of international crime syndicates; intelligence on certain types of crime directed against public and national security (e.g. domestic insurrection, foreign aggression) and intelligence related to the task of ensuring cyber security and preventing or countering cyberattacks and threats (Article 4(2) NIS Act). See also Annex II, section 3.1.

322 See also Articles 14, 22 and 23 NIS Act.

323 Article 4(2) NIS Act.

324 Articles 3(1), 6(2), 11, 21 NIS Act. See also the rules on conflicts of interest, in particular Articles 10, 12 NIS Act.

any institution, organisation or individual to do anything they are not obligated to do (under law), nor obstruct any person's exercise of his or her rights[325].

3.3.1.1 Access to communication information

(187) On the basis of the CPPA, Korean public authorities[326] may collect communication confirmation data (i.e. the date of telecommunications, their start- and end-time, the number of outgoing and incoming calls as well as the subscriber number of the other party, the frequency of use, log files on the use of telecommunication services and location information, see recital (155)) and the content of communications (by means of communication-restricting measures, see recital (155)) for national security purposes (as determined by the mandate of the NIS, see footnote 322 earlier). These powers extend to two types of information: (1) communications to which one or both parties are Korean nationals[327]; and (2) communications of a) countries hostile to the Republic of Korea, b) foreign agencies, groups or nationals suspected of engaging in anti-Korean activities[328], or c) members of groups operating within the Korean Peninsula but effectively beyond the sovereignty of the Republic of Korea and their umbrella groups based in foreign countries[329]. Communications of EU individuals transferred from the Union to the Republic of Korea on the basis of this Decision can therefore only be collected under the CPPA for national security purposes (subject to the conditions set out in recitals (188) - (192)) if, either, they are between an EU individual and a Korean national, or, if they concern communications exclusively between non-Korean nationals, fall within one of the three mentioned categories 2a), b) and c).

(188) In both scenarios, the collection of communication confirmation data may only take place for the purpose of preventing threats to national security[330] while communication-restricting measures may only be taken when there is a grave risk to national security and the collection is necessary to prevent it[331]. In addition, the content of communications may only be accessed as a measure of last resort and efforts must be made to minimize the violation of the privacy of communications[332], thereby ensuring that it remains proportionate to the national security objective pursued. The collection of both the content of communications and communication confirmation data may only last for a maximum period of four months, and must be discontinued immediately if the pursued objective is achieved earlier[333]. If the relevant conditions continue to be fulfilled, the period may be extended, with the prior

325 Article 13 NIS Act.

326 This includes the intelligence agencies (i.e. the NIS and Defense Security Support Command) and the police/prosecution.

327 Article 7(1)1 CPPA.

328 As explained by the Korean government in footnote 244 of Annex II, this refers to activities that threaten the nation's existence and safety, democratic order or the people's survival and freedom.

329 Article 7(1)2 CPPA.

330 Article 13-4 CPPA.

331 Article 7(1) CPPA.

332 Article 3(2) CPPA. In addition, communication-restricting measures must be discontinued immediately once they are no longer necessary, thereby ensuring that any infringement of the individual's communication secrets is limited to the minimum (Article 2 CPPA Enforcement Decree).

333 Article 7(2) CPPA.

permission of a court (for the measures described in recital (189)) or the President (for the measures described in recital (190))[334], for up to four months.

(189) The same procedural safeguards apply to the collection of communication confirmation data and the content of communications[335]. In particular, where at least one of the individuals involved in the communication is a Korean national, the intelligence agency must submit a written request to the High Prosecutors' Office, which in turn must apply for a warrant from a senior Chief Justice of the High Court[336]. The CPPA lists the information that must be provided in the request to the Prosecutor, the application for the warrant and the warrant itself, which includes, in particular, the justification for the request and main grounds for suspicion, supporting materials, as well as information on the objective, target (i.e. the targeted individual(s)), scope and duration of the proposed measure[337]. Warrantless collection may only take place if there is an act of conspiracy that threatens national security and an emergency exists that makes it impossible to go through the aforementioned procedures[338]. However, also in that case an application for a warrant must be filed immediately after the measure is taken[339]. The CPPA therefore clearly defines the scope and conditions of these types of collection, and subjects them to specific (procedural) safeguards (including prior judicial approval), which ensures that the use of such measures is limited to what is necessary and proportionate. Moreover, the requirement to provide detailed information in both the application for a warrant and the warrant itself rules out the possibility of indiscriminate access.

(190) For communications between non-Korean nationals that fall within one of the three specific categories listed in recital (187), an application must be filed with the Director of the NIS, who, after a review of the appropriateness of the proposed measures, must request prior written approval from the President of the Republic of Korea[340]. The application prepared by the intelligence agency must include the same detailed information as an application for a court warrant (see recital (189)), in particular on the justification for the request and the main grounds for suspicion, supporting materials and information on the objectives, targeted individual(s), scope and duration of the

---

334 The application to obtain approval to extend the surveillance measures must be made in writing, stating the reasons why extension is sought and providing supporting materials (Article 7(2) CPPA and Article 5 CPPA Enforcement Decree).

335 See Article 13-4(2) CPPA and Article 37(4) CPPA Enforcement Decree, according to which the procedures applicable to the collection of the content of communications also apply to the collection of communication confirmation data. See also Annex II, section 3.2.1.1.1.

336 Articles 6(5), (8) and 7(1)1, (3) and CPPA in conjunction with Article 7(3)-(4) CPPA Enforcement Decree.

337 See Articles 7(3) and 6(4) CPPA (for the request from the intelligence agency), Article 4 CPPA Enforcement Decree (for the application by the Prosecutor) and Articles 7(3) and 6(6) CPPA (for the warrant).

338 Article 8 CPPA.

339 Article 8(2) and (8) CPPA. The collection must be discontinued immediately if court permission is not obtained within 36 hours from the time the measures are taken. In cases where the surveillance is completed within a short time, ruling out court permission, the head of the competent High Prosecutors' Office must send an emergency measure notice prepared by the intelligence agency to the head of the competent court, which on this basis can examine the legality of the collection (Article 8(5) and (7) CPPA). This notice must indicate the objective, target, scope, period, place of execution and method of surveillance, as well as the grounds for not filing a request before taking the measure (Article 8(6) CPPA). More generally, intelligence agencies may only take emergency measures in accordance with an "emergency censorship/wiretapping statement" and must keep records of such measures (Article 8(4) CPPA).

340 Article 8(1), (2) CPPA Enforcement Decree.

proposed measures[341]. In emergency situations[342], prior approval from the Minister to whom the relevant intelligence agency belongs must be obtained, although the intelligence agency must apply for the approval of the President immediately after the emergency measures have been taken[343]. Also with respect to the collection of communications between exclusively non-Korean nationals, the CPPA therefore limits the use of such measures to what is necessary and proportionate, by clearly circumscribing the limited categories of individuals that may be subject to such measures and by laying down detailed criteria that intelligence agencies have to demonstrate to justify an application for the collection of information. Moreover, this again rules out the possibility of indiscriminate access. While there is no prior independent approval of such measures, independent oversight is ensured ex post by, in particular, the PIPC and NHRC (see for instance recitals (199) - (200)).

(191) The CPPA furthermore imposes several additional safeguards that contribute to ex post oversight and facilitate individuals' access to effective remedies. Firstly, with respect to any type of collection for national security purposes, the CPPA provides for different record-keeping and reporting requirements. In particular, when requesting the cooperation of private operators, intelligence agencies have to provide the court warrant/presidential permission or a copy of the cover of an emergency censorship statement, which the compelled entity must keep in its files[344]. Where private operators are compelled to cooperate, records must be kept by both the requesting public authority and the relevant operator on the purpose and object of the measures, as well as the date of execution[345]. In addition, intelligence agencies have to report on the information they have gathered and the outcome of the surveillance activity to the Director of the NIS[346].

(192) Secondly, individuals have to be notified about the collection of their data (communication confirmation data or the content of communications) for national security purposes if it concerns communications where at least one of the parties is a Korean national[347]. This notification must be provided in writing within 30 days from the date on which the collection ended (including where the data was obtained in accordance with the emergency procedure) and may only be deferred if and as long as

---

341 Article 8(3) CPPA Enforcement Decree in conjunction with Article 6(4) CPPA.

342 That is, in cases when the measure aims at an act of conspiracy that threatens national security, there is insufficient time to obtain approval of the President and failure to adopt emergency measures may harm national security (Article 8(8) CPPA).

343 Article 8(9) CPPA. The collection must immediately be discontinued if the permission is not obtained within 36 hours from the point in time the application is made.

344 Article 9(2) CPPA and Article 12 CPPA Enforcement Decree. See Article 13 CPPA Enforcement Decree on the possibility to compel the assistance of post offices and telecommunication service providers. Private operators requested to disclose information may refuse to do so when the warrant/authorisation or emergency censorship statement refers to the wrong identifier (e.g. a telephone number belonging to a different individual than the one identified). In any event, they are prohibited from disclosing passwords used for communications (Article 9(4) CPPA).

345 For communication-restricting measures, such records must be kept for three years, see Article 9(3) CPPA and Article 17(2) CPPA Enforcement Decree. With respect to communication confirmation data, intelligence agencies must keep records of the fact that a request for such data was made, as well as of the written request itself and the institution that relied on it (Article 13(5) and 13-4(3) CPPA). Telecommunication service providers have to keep records for seven years and report twice per year to the Minister of Science and ICT on the frequency of such disclosures (Article 9(3) CPPA in conjunction with Article 13(7) CPPA and Articles 37(4) and 39 CPPA Enforcement Decree).

346 Article 18(3) CPPA Enforcement Decree.

347 Articles 9-2(3) and 13-4 CPPA. The notification must include (1) the fact that the information has been collected, (2) the executing agency and (3) the execution period.

it would put national security at risk or would harm people's life and physical safety[348]. Irrespective of such notification, individuals may obtain redress via different avenues, as explained in more detail in section 3.3.4.

3.3.1.2 Collection of information on terrorist suspects

(193) The Anti-Terrorism Act provides that the NIS may collect data on terrorist suspects[349] in accordance with the limitations and safeguards laid down in other laws[350]. In particular, the NIS may obtain communications data (on the basis of the CPPA) and other personal information (through a request for voluntary disclosure)[351]. With respect to the collection of communications information (i.e. the content of communications or communication confirmation data), the limitations and safeguards described in section 3.3.1.1 apply, including the requirement of obtaining a court approved warrant. As regards requests for voluntary disclosure of other types of personal data of terrorist suspects, the NIS must comply with the requirements under the Constitution and PIPA on necessity and proportionality (see recital (164))[352]. Controllers receiving such requests may comply on a voluntary basis under the conditions set out in PIPA (for instance in accordance with the principle of data minimisation and by limiting the impact on the privacy of the individual)[353]. In this case, they also have to comply with the requirement to notify the concerned individual following from Notification No 2021-5 (see recital (166)).

3.3.1.3 Requests for voluntary disclosure of subscriber data

---

348 Article 9-2(4) CPPA. In that case, the notification must be given within 30 days once the grounds for deferral cease to exist, see Articles 13-4(2) and 9-2(6) CPPA.

349 That is, members of a terrorist group (as designated by the United Nations, see Article 2(2) Anti-Terrorism Act.); persons who promote and disseminate ideas or tactics of a terrorist group, raise or contribute to funds for terrorism, or engage in other activities of preparing, conspiring, propagandizing, or instigating terrorism; or persons for which there are good grounds to suspect that they have performed such activities (Article 2(3) Anti-Terrorism Act). "Terrorism" is defined by Article 2(1) Anti-Terrorism Act as conduct carried out for the purpose of impeding the exercise of the authority of the State, a local government or a foreign government (including international organisations), or for the purpose of forcing it to take action without any legal obligation to do so, or threatening the public. Such conduct may for example include killing, kidnapping, or taking a person hostage; hijacking/seizing, destroying or damaging a ship or aircraft; using biochemical, explosive or incendiary weapons with the intention of causing death, serious injury or damage; and abusing nuclear or radioactive materials.

350 Article 9(1) and (3) Anti-Terrorism Act.

351 While the Anti-Terrorism Act also refers to the possibility of collecting information on the entry into and departure from the Republic of Korea on the basis of the Immigration Act and Customs Act, those laws currently do not provide for such an empowerment (see section 3.2.2.1 of Annex II). In any event, they would in principle not apply to data transferred on the basis of this Decision, as they would typically concern information that would be collected directly by the Korean authorities (rather than access to data that was previously transferred from the Union to Korean controllers). In addition, the Anti-Terrorism Act lists the ARUSFTI as a legal basis for the collection of information on financial transactions. However, as explained in footnote 200, the types of data that could be obtained on the basis of this Act does not fall within the scope of this Decision. Finally, the Anti-Terrorism Act also provides that the NIS may collect location information through non-binding requests, in which case location information providers could voluntarily disclose such information under the conditions set out in PIPA (as described in recital (193)) and the Location Information Act. However, as also explained in footnote 17, location information would not be transferred from the Union to Korean controllers on the basis of this Decision, but would rather be generated inside Korea.

352 See Annex II, section 3.2.2.2.

353 See Article 58(4) PIPA, which requires that personal information is processed to the minimum extent necessary to attain the intended purpose, and Article 3(6) PIPA, which provides that personal information must be processed in a manner to minimise the possibility of infringing on the privacy of the individual. See also Article 59 lit. 2, 3 PIPA, according to which controllers are prohibited from disclosing personal information to third parties without authority.

(194) On the basis of the TBA, telecommunication providers may voluntarily disclose subscriber data (see recital (163)) upon request of an intelligence agency that intends to collect such information to prevent a threat to national security[354]. As regards such requests from the NIS, the same limitations (following from the Constitution, PIPA and the TBA) apply as in the area of criminal law enforcement, as set out in recital (164)[355]. Telecommunication providers are not required to comply and can only do so under the conditions set out in PIPA (in particular in accordance with the principle of data minimisation and by limiting the impact on the privacy of the individual, see also recital (193)). The same requirements with respect to record-keeping and notification of the concerned individual apply as in the area of criminal law enforcement (see recitals (165) and (166)).

3.3.2 Further use of the information collected

(195) The processing of personal data collected by Korean authorities for national security purposes is subject to the principles of purpose limitation (Article 3(1)-(2) PIPA), lawfulness and fairness of processing (Article 3(1) PIPA), proportionality/data minimisation (Articles 3(1), (6) and 58 PIPA), accuracy (Article 3(3) PIPA), transparency (Article 3(5) PIPA), security (Article 58(4) PIPA) and storage limitation (Article 58(4) PIPA)[356]. Possible disclosure of personal data to third parties (including third countries) can only take place in accordance with these principles (in particular purpose limitation and data minimisation), after having assessed compliance with the principles of necessity and proportionality (Article 37(2) of the Constitution) and taking into account the impact on the rights of the individuals concerned (Article 3(6) PIPA).

(196) As regards the content of communications and communication confirmation data, the CPPA further limits the use of such data to judicial proceedings, where a party relating to the communication relies on them in a claim for damages; or allowed uses under other laws[357].

3.3.3 Oversight

(197) The activities of Korean national security authorities are supervised by different bodies[358].

(198) Firstly, the Anti-Terrorism Act provides for specific oversight mechanisms for counterterrorism activities, including the collection of data on terrorism suspects. In particular, at the level of the executive, counterterrorism activities are overseen by the Counterterrorism Commission[359], to which the Director of the NIS is required to report on investigations and the tracing of terrorist suspects to collect information or materials necessary for counterterrorism activities[360]. In addition, the Human Rights Protection Officer (HRPO) specifically oversees compliance of counterterrorism activities with fundamental rights[361]. The HRPO is appointed by the Chairperson of

354 Article 83(3) TBA.

355 See also Annex II, section 3.2.3.

356 See Annex II, section 1.2.

357 Articles 5(1)-(2), 12 and 13-5 CPPA.

358 See Annex II, section 3.3.

359 Article 5(3) Anti-Terrorism Act. The Commission is chaired by the Prime Minister and comprised of several ministers and heads of governmental agencies, such as the Ministers of Foreign Affairs, Justice, National Defense, and Interior and Safety, the Director of the NIS and the Commissioner General of the National Police Agency (Article 3(1) Anti-Terrorism Act Enforcement Decree).

360 Article 9(4) Anti-Terrorism Act.

361 Article 7 Anti-Terrorism Act.

the Counterterrorism Commission among individuals that meet specific qualifications listed in the Enforcement Decree of the Anti-Terrorism Act[362] for a (renewable) term of two years and may only be removed from office on specific, limited grounds and for good cause[363]. In exercising its oversight function, the HRPO may issue general recommendations for improving the protection of human rights[364] and specific recommendations for corrective measures if a human rights violation has been established[365]. Public authorities are required to inform the HRPO of the follow-up provided to its recommendations[366].

(199) Secondly, the PIPC oversees compliance by national security authorities with data protection rules, which includes both the applicable provisions of PIPA (see recital (149)) and the limitations and safeguards that apply to the collection of personal data under other laws (the CPPA, Anti-Terrorism Act and TBA, see also recital (171))[367]. In exercising this oversight role, the PIPC can make use of all of its investigatory and remedial powers, as described in detail in section 2.4.2.

(200) Thirdly, the activities of national security authorities are subject to the independent oversight of the NHRC, in accordance with the procedures described in recital (172)[368].

(201) Fourthly, the oversight function of the BAI also extends to national security authorities, although the NIS may, in exceptional circumstances, refuse to provide certain information or materials, i.e. when they constitute state secrets and public knowledge would have a serious impact on national security[369].

(202) Finally, parliamentary oversight of the activities of the NIS is carried out by the National Assembly (through a specialised Intelligence Committee)[370]. The CPPA establishes a specific oversight role for the National Assembly with respect to the use of communication-restricting measures for national security purposes[371]. In particular,

---

362 That is, anyone qualified as an attorney-at-law with at least ten years working experience, or with expert knowledge in the field of human rights and serving or having served (at least) as an associate professor for at least ten years, or having served as a higher public official in State agencies or local governments, or with at least ten years working experience in the field of human rights, e.g. in a non-governmental organisation (Article 7(1) Anti-Terrorism Act Enforcement Decree).

363 For instance, when indicted in a criminal case related to his/her duties, when divulging confidential information, or because of long-term mental or physical incapacity (Article 7(3) Anti-Terrorism Act Enforcement Decree).

364 Article 8(1) Anti-Terrorism Act Enforcement Decree.

365 Article 9(1) Anti-Terrorism Act Enforcement Decree. The HRPO decides autonomously on the adoption of recommendations, but is required to report such recommendations to the Chairperson of the Counterterrorism Commission.

366 Article 9(2) Anti-Terrorism Act Enforcement Decree. According to the official representation of the Korean government, a failure to implement a recommendation of the HRPO would be elevated to the Counterterrorism Commission, including the Prime Minister, although so far there have been no cases where HRPO recommendations have not been implemented (see section 3.3.1 of Annex II).

367 Annex II, section 3.3.4.

368 Specifically with respect to the NIS, the NHRC has in the past carried out ex officio investigations and handled a number of individual complaints. See e.g. the NHRC's annual report 2018, p. 128 (available at https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746) and the NHRC's annual report 2019, p. 70 (available at https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

369 Article 13(1) NIS Act.

370 Articles 36 and 37(1)15 National Assembly Act.

371 Article 15 CPPA.

the National Assembly may conduct on-the-spot inspections of wiretapping equipment and may require both the NIS and telecommunication operators that have disclosed the content of communications to report thereon. The National Assembly may also carry out its general oversight functions (in accordance with the procedures described in recital (174)). The NIS Act requires the Director of the NIS to respond without delay when the Intelligence Committee requests a report on a specific matter[372], with specific rules for certain particularly sensitive information. Concretely, the Director of the NIS may only refuse to reply or testify before the Committee in exceptional circumstances, i.e. if the request relates to state secrets concerning military, diplomatic or North Korea-related issues where public knowledge could have a serious impact on the country's "national destiny"[373]. In this case, the Intelligence Committee may request an explanation from the Prime Minister and, if no explanation is provided within seven days, the reply or testimony may not be refused.

3.3.4 Redress

(203) Also in the area of national security, the Korean system offers different (judicial) avenues to obtain redress, including compensation for damages. These mechanisms provide data subjects with effective administrative and judicial remedies, enabling them in particular to enforce their rights, including the right to have access to their personal data, or to obtain the rectification or erasure of such data.

(204) Firstly, pursuant to Articles 3(5) and 4(1), (3) and (4) PIPA, individuals can exercise their rights of access, correction, deletion and suspension vis-à-vis national security authorities. Section 6 of Notification No 2021-5 (Annex I to this Decision) further clarifies how these rights apply in the context of data processing for national security purposes. In particular, a national security authority may only limit or deny the exercise of the right to the extent and for as long as necessary and proportionate to protect an important objective of public interest (for instance to the extent that, and for as long as, granting the right would jeopardise an ongoing investigation or threaten national security), or where granting the right may cause damage to the life or body of a third party. Invoking such a restriction therefore requires a balancing of the rights and interests of the individual against the relevant public interest and may not, in any event, affect the essence of the right (Article 37(2) of the Constitution). Where the request is denied or restricted, the individual must be notified of the reasons without delay.

(205) Secondly, individuals have a right to obtain redress under PIPA if their data has been processed by a national security authority in violation of PIPA or the limitations and safeguards in other laws governing the collection of personal data (in particular the CPPA, see recital (171))[374]. This right can be exercised through a complaint to the PIPC (including via the Privacy Call Centre operated by the Korea Internet and Security Agency)[375]. Moreover, to facilitate easier access to redress against Korean national security authorities, EU individuals may submit a complaint to the PIPC through their national data protection authority.[376] In this case, the PIPC will notify the individual via the national data protection authority once the investigation is

372 Article 15(2) NIS Act.

373 Article 17(2) NIS Act. "State secrets" are defined as (classified) facts, goods or knowledge which shall not be disclosed to any other country or organization in order to avoid any serious disadvantage to the national safety, and to which only limited access is permitted. See Article 13(4) NIS Act.

374 Articles 58(4) and 4(5) PIPA. See Annex II, section 3.4.2.

375 Articles 62 and 63(2) PIPA.

376 Notification No 2021-5 (Section 6, Annex I).

concluded (including, where applicable, with information about the corrective measures imposed). On the basis of the Administrative Litigation Act, individuals may furthermore appeal/challenge the decisions or inaction of the PIPC (see recital (132)).

(206) Thirdly, individuals may lodge a complaint with the HRPO about the infringement of their right to privacy/data protection in the context of counterterrorism activities (i.e. pursuant to the Anti-Terrorism Act)[377], which can recommend corrective action. As there are no admissibility requirements before the HRPO, a complaint will be handled even if the concerned individual cannot demonstrate that (s)he has in fact been injured (for instance because of the alleged unlawful collection of his/her data by a national security authority)[378]. The relevant authority must inform the HRPO of any measures taken to implement its recommendations.

(207) Fourthly, individuals may lodge a complaint with the NHRC concerning the collection of their data by national security authorities and obtain redress in accordance with the procedure described in recital (178)[379].

(208) Finally, different judicial remedies are available[380], allowing individuals to invoke the limitations and safeguards described in section 3.3.1 to obtain redress. In particular, individuals may challenge the legality of actions of national security authorities on the basis of the Administrative Litigation Act (in accordance with the procedure described in recital (181) or the Constitutional Court Act (see recital (182)). In addition, they may obtain compensation for damages on the basis of the State Compensation Act (as described in more detail in recital (183)).

4. CONCLUSION

(209) The Commission considers that the Republic of Korea – through PIPA, the special rules applicable to certain sectors (as analysed in Section 2) and the additional safeguards provided in Notification No 2021-5 (Annex I) – ensures a level of protection for personal data transferred from the European Union that is essentially equivalent to the one guaranteed by Regulation (EU) 2016/679.

(210) Moreover, the Commission considers that, taken as a whole, the oversight mechanisms and redress avenues in Korean law enable infringements of the data protection rules by controllers in Korea to be identified and addressed in practice and offer legal remedies to the data subject to obtain access to his/her personal data and, eventually, the rectification or erasure of such data..

(211) Finally, on the basis of the available information about the Korean legal order, including the representations, assurances and commitments from the Korean government contained in Annex II, the Commission considers that any interference in the public interest, in particular criminal law enforcement and national security purposes, by Korean public authorities with the fundamental rights of individuals whose personal data are transferred from the European Union to the Republic of Korea

377 Article 8(1) lit 2 Anti-Terrorism Act Enforcement Decree.

378 See Annex II, section 3.4.1.

379 For example, the NHRC regularly receives complaints against the National Intelligence Service, see the figures in the NHRC's annual report 2019 on the number of complaints received between 2015 and 2019, p. 70 (available at https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

380 See Annex II, section 3.4.4.

will be limited to what is strictly necessary to achieve the legitimate objective in question, and that effective legal protection against such interference exists.

(212) Therefore, in the light of the findings of this Decision, it should be decided that the Republic of Korea ensures an adequate level of protection within the meaning of Article 45 of Regulation (EU) 2016/679, interpreted in light of the Charter of Fundamental Rights of the European Union, for personal data transferred from the European Union to the Republic of Korea to personal information data controllers in the Republic of Korea subject to PIPA, with the exception of religious organisations to the extent they process personal data for their missionary activities; political parties to the extent they process personal data in the context of the nomination of candidates and controllers that are subject to oversight by the Financial Services Commission for the processing of personal credit information pursuant to the Credit Information Act, to the extent they process such information.

5. EFFECTS OF THIS DECISION AND ACTION OF DATA PROTECTION AUTHORITIES

(213) Member States and their organs are required to take the measures necessary to comply with acts of the Union institutions, as the latter are presumed to be lawful and accordingly produce legal effects until such time as they are withdrawn, annulled in an action for annulment or declared invalid following a reference for a preliminary ruling or a plea of illegality.

(214) Consequently, a Commission adequacy decision adopted pursuant to Article 45(3) of Regulation (EU) 2016/679 is binding on all organs of the Member States to which it is addressed, including their independent supervisory authorities. In particular, transfers from a controller or processor in the European Union to controllers in the Republic of Korea may take place without the need to obtain any further authorisation.

(215) It should be recalled that, pursuant to Article 58(5) of Regulation (EU) 2016/679 and as explained by the Court of Justice in the *Schrems* judgment[381], where a national data protection authority questions, including upon a complaint, the compatibility of a Commission adequacy decision with the fundamental rights of the individual to privacy and data protection, national law must provide it with a legal remedy to put those objections before a national court which may be required to make a reference for a preliminary ruling to the Court of Justice[382].

6. MONITORING AND REVIEW OF THIS DECISION

(216) According to the case law of the Court of Justice,[383] and as recognised in Article 45(4) of Regulation (EU) 2016/679, the Commission should continuously monitor relevant developments in the third country after the adoption of an adequacy decision in order to assess whether the third country still ensures an essentially equivalent level of protection. Such a check is required, in any event, when the Commission receives information giving rise to a justified doubt in that respect.

---

381 *Schrems*, paragraph 65.

382 *Schrems*, paragraph 65: "It is incumbent upon the national legislature to provide for legal remedies enabling the national supervisory authority concerned to put forward the objections which it considers well founded before the national courts in order for them, if they share its doubts as to the validity of the Commission decision, to make a reference for a preliminary ruling for the purpose of examination of the decision's validity."

383 *Schrems*, paragraph 76.

(217) Therefore, the Commission should on an on-going basis monitor the situation in the Republic of Korea as regards the legal framework and actual practice for the processing of personal data as assessed in this Decision, including compliance by the Korean authorities with the representations, assurances and commitments contained in Annex II. To facilitate this process, the Korean authorities are invited to promptly inform the Commission of material developments relevant to this Decision, as regards the processing of personal data by business operators and public authorities, as well as the limitations and safeguards applicable to access to personal data by public authorities.

(218) Moreover, in order to allow the Commission to effectively carry out its monitoring function, the Member States should inform the Commission about any relevant action undertaken by the national data protection authorities, in particular regarding queries or complaints by EU data subjects concerning the transfer of personal data from the European Union to data controllers in the Republic of Korea. The Commission should also be informed about any indications that the actions of Korean public authorities responsible for the prevention, investigation, detection or prosecution of criminal offences, or for national security, including any oversight bodies, do not ensure the required level of protection.

(219) In application of Article 45(3) of Regulation (EU) 2016/679[384], and in the light of the fact that the level of protection afforded by the Korean legal order may be liable to change, the Commission, following the adoption of this Decision, should periodically review whether the findings relating to the adequacy of the level of protection ensured by the Republic of Korea are still factually and legally justified.

(220) To this end, this Decision should be subject to a first review within three years after its entry into force. Following that first review, and depending on its outcome, the Commission will decide in close consultation with the Committee established under Article 93(1) of Regulation (EU) 2016/679 whether the three-year-cycle should be maintained. In any case, the subsequent reviews should take place at least every four years[385]. The review should cover all aspects of the functioning of this Decision, and in particular the application of the additional safeguards contained in Annex I to this Decision, with special attention paid to protections afforded in case of onward transfers; relevant case law developments; the rules on the processing of pseudonymised information for purposes of statistics, scientific research and archiving in the public interest, as well as the application of the exceptions under Article 28(7) PIPA; the effectiveness of the exercise of individual rights, including before the recently reformed PIPC, and the application of exceptions to those rights; the application of the partial exemptions under PIPA; as well as the limitations and safeguards with respect to government access (as set out in Annex II to this Decision), including the cooperation of the PIPC with EU data protection authorities on complaints from individuals. It should also cover the effectiveness of oversight and enforcement, as regards PIPA and in the area of criminal law enforcement and national security (in particular by the PIPC and NHRC).

(221) To perform the review, the Commission should meet with the PIPC, accompanied, where appropriate, by other Korean authorities responsible for government access,

---

384 According to Article 45(3) Regulation (EU) 2016/679, "[t]he implementing act shall provide for a mechanism for a periodic review, […] which shall take into account all relevant developments in the third country or international organisation."

385 Article 45(3) Regulation (EU) 2016/679 provides that a periodic review must take place "at least every four years". See also European Data Protection Board, Adequacy Referential, WP 254 rev. 01.

including relevant oversight bodies. The participation in this meeting should be open to representatives of the members of the European Data Protection Board. In the framework of the review, the Commission should request the PIPC to provide comprehensive information on all aspects relevant for the adequacy finding, including on the limitations and safeguards concerning government access[386]. The Commission should also seek explanations on any information relevant for this Decision that it has received, including public reports by Korean authorities or other stakeholders in Korea, the European Data Protection Board, individual data protection authorities, civil society groups, media reports, or any other available source of information.

(222) On the basis of the review, the Commission should prepare a public report to be submitted to the European Parliament and the Council.

7. SUSPENSION, REPEAL OR AMENDMENT OF THIS DECISION

(223) Where available information, in particular information resulting from the monitoring of this Decision or provided by Korean or Member States' authorities, reveals that the level of protection afforded by the Republic of Korea may no longer be adequate, the Commission should promptly inform the competent Korean authorities thereof and request that appropriate measures be taken within a specified, reasonable timeframe.

(224) If, at the expiry of that specified timeframe, the competent Korean authorities fail to take those measure or otherwise demonstrate satisfactorily that this Decision continues to be based on an adequate level of protection, the Commission will initiate the procedure referred to in Article 93(2) of Regulation (EU) 2016/679 with a view to partially or completely suspend or repeal this Decision.

(225) Alternatively, the Commission will initiate that procedure with a view to amend the Decision, in particular by subjecting data transfers to additional conditions or by limiting the scope of the adequacy finding only to data transfers for which an adequate level of protection continues to be ensured.

(226) In particular, the Commission should initiate the procedure for suspension or repeal in case of indications that the additional safeguards contained in Annex I are not complied with by business operators receiving personal data under this Decision and/or are not effectively enforced, or that the Korean authorities fail to comply with the representations, assurances and commitments contained in Annex II to this Decision.

(227) The Commission should also consider initiating the procedure leading to the amendment, suspension or repeal of this Decision if, in the context of the review or otherwise, the competent Korean authorities fail to provide the information or clarifications necessary for the assessment of the level of protection afforded to personal data transferred from the European Union to the Republic of Korea, or as regards compliance with this Decision. In this respect, the Commission should take into account the extent to which the relevant information can be obtained from other sources.

(228) On duly justified imperative grounds of urgency, the Commission will make use of the possibility to adopt, in accordance with the procedure referred to in Article 93(3) of Regulation (EU) 2016/679, immediately applicable implementing acts suspending, repealing or amending the Decision.

386 See Annex II to this Decision.

8. FINAL CONSIDERATIONS

(229) The European Data Protection Board published its opinion[387], which has been taken into consideration in the preparation of this Decision.

(230) The measures provided for in this Decision are in accordance with the opinion of the Committee established under Article 93(1) Regulation (EU) 2016/679.

HAS ADOPTED THIS DECISION:

Article 1

1. For the purpose of Article 45 of Regulation (EU) 2016/679, the Republic of Korea ensures an adequate level of protection for personal data transferred from the European Union to entities in the Republic of Korea subject to the Personal Information Protection Act as complemented by the additional safeguards set out in Annex I, together with the official representations, assurances and commitments contained in Annex II.

2. This Decision does not cover personal data transferred to recipients falling within one of the following categories, to the extent all or part of the purposes of processing of the personal data corresponds to one of the purposes listed therein, respectively:

   (a) religious organisations to the extent they process personal data for their missionary activities;

   (b) political parties to the extent they process personal data in the context of the nomination of candidates;

   (c) entities that are subject to oversight by the Financial Services Commission for the processing of personal credit information pursuant to the Credit Information Act, to the extent they process such information.

Article 2

Whenever the competent authorities in Member States, in order to protect individuals with regard to the processing of their personal data, exercise their powers pursuant to Article 58 of Regulation (EU) 2016/679 with respect to data transfers falling within the scope of application set out in Article 1 of this Decision, the Member State concerned shall inform the Commission without delay.

Article 3

1. The Commission shall continuously monitor the application of the legal framework upon which this Decision is based, including the conditions under which onward transfers are carried out, individual rights are exercised and Korean public authorities have access to data transferred on the basis of this Decision, with a view to assessing whether the Republic of Korea continues to ensure an adequate level of protection within the meaning of Article 1.

[387] Opinion 32/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the Republic of Korea, available at the following link: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-322021-regarding-european-commission-draft_en.

2. The Member States and the Commission shall inform each other of cases where the Personal Information Protection Commission, or any other competent Korean authority, fails to ensure compliance with the legal framework upon which this Decision is based.

3. The Member States and the Commission shall inform each other of any indications that interferences by Korean public authorities with the right of individuals to the protection of their personal data go beyond what is strictly necessary, or that there is no effective legal protection against such interferences.

4. After three years from the date of the notification of this Decision to the Member States and subsequently at least every four years, the Commission shall evaluate the finding referred to in Article 1(1) on the basis of all available information, including the information received as part of the review carried out together with the relevant Korean authorities.

5. Where the Commission has indications that an adequate level of protection is no longer ensured, the Commission shall inform the competent Korean authorities. If necessary, it may decide to suspend, amend or repeal this Decision, or limit its scope, in accordance with Article 45(5) of Regulation (EU) 2016/679, in particular where it has indications that:

   (a) controllers in Korea that have received personal data from the European Union under this Decision do not comply with the additional safeguards contained in Annex I, or there is insufficient oversight and enforcement in this regard;

   (b) the Korean public authorities do not comply with the representations, assurances and commitments contained in Annex II, including as regards the conditions and limitations for the collection of and access to personal data transferred under this Decision by Korean public authorities for criminal law enforcement or national security purposes.

   The Commission may also adopt such measures if the lack of cooperation of the Korean government prevents the Commission from determining whether the Republic of Korea continues to ensure an adequate level of protection.

Article 4

This Decision is addressed to the Member States.

Done at Brussels, 17.12.2021

For the Commission
Didier REYNDERS
Member of the Commission

CERTIFIED COPY
For the Secretary-General

Martine DEPREZ
Director
Decision-making & Collegiality
EUROPEAN COMMISSION

EUROPEAN
COMMISSION

Brussels, 17.12.2021
C(2021) 9316 final

ANNEXES 1 to 2

ANNEXES

to the

COMMISSION IMPLEMENTING DECISION

pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the Republic of Korea under the Personal Information Protection Act

ANNEX I

SUPPLEMENTARY RULES FOR THE INTERPRETATION AND APPLICATION OF THE PERSONAL INFORMATION PROTECTION ACT RELATED TO THE PROCESSING OF PERSONAL DATA TRANSFERRED TO KOREA

Contents

I. Outline

Korea and the European Union (hereinafter referred to as the 'EU') have been engaged in adequacy discussions, as a result of which the European Commission determined that Korea is guaranteeing an adequate level of personal data protection according to Article 45 of GDPR.

In this context, the Personal Information Protection Commission adopted this Notification based on Article 5 (Obligations of State, etc) and Article 14 (International Cooperation)[1] of the Personal Information Protection Act to clarify the interpretation, application and enforcement of certain provisions of the Act, including in regard to the processing of personal data transferred to Korea based on the EU adequacy decision.

As this Notification has the status of an administrative rule that the competent administrative agency establishes and announces to clarify the standards for interpreting, applying and

[1] Article 14 of the「Personal Information Protection Act」stipulates the Korean Government's authority to establish policies to improve the level of personal information protection in the international environment and prevent the infringement of the rights of data subjects due to the cross-border transfer of personal information.

enforcing the 「Personal Information Protection Act」 in the legal system of Korea, it has legally binding force on the personal information controller in the sense that any violation of this Notification may be regarded as a violation of the relevant provisions of PIPA. In addition, if personal rights and interests are infringed due to a violation of this Notification, relevant individuals are entitled to obtain redress from the Personal Information Protection Commission or the court.

Accordingly, if the personal information controller, who processes the personal information transferred to Korea according to the EU adequacy decision, fails to take measures conforming to this Notification, it will be deemed "that there is substantial ground to deem that there has been an infringement with respect to personal information, and failure to take action is likely cause damage that is difficult to remedy", pursuant to Paragraphs 1 and 2 of Article 64 of the Act. In such cases, the Personal Information Protection Commission or related central administrative agencies may order the relevant personal information controller to take corrective measures, etc. according to the authority given by this provision, and, depending on specific violations of the law, corresponding punishment (penalties, administrative fines, etc.) may be imposed as well.

II. Definition of terms

The definitions of the terms used in this provision are as follows:

(i) Act: Personal Information Protection Act (Act No. 16930, amended on February 4, 2020, and enforced on August 5, 2020)

(ii) Presidential Decree: Enforcement Decree of the Personal Information Protection Act (Presidential Decree No. 30509, 03. Mar, 2020., Amends Other Acts)

(iii) Data subject: an individual who is identifiable by the information processed hereby to become the subject of that information

(iv) Personal information controller: a public institution, legal person, organization, individual, etc. that processes personal information directly or indirectly as part of its activities;

(v) EU: EU (As of the end of February 2020, 27 member countries[2], including Belgium, Germany, France, Italy, Luxemburg, the Netherlands, Denmark, Ireland, Greece, Portugal, Spain, Austria, Finland, Sweden, Cyprus, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Slovakia, Slovenia, Rumania, Bulgaria and Croatia) as well as countries associated to the EU through the EEA Agreement (Iceland, Liechtenstein, Norway).

(vi) GDPR: The EU's general personal information protection law, General Data Protection Regulation (Regulation EU 2016/679)

(vii) Adequacy decision: According to Paragraph 3 of Article 45 of GDPR, the European Commission decided that a third country, the territory of a third country, one or more areas or an international organization guarantees an adequate level of personal information protection.

III. Supplementary rules

[2] Until the end of the transition period, this also includes the United Kingdom, as provided by Articles 126, 127 and 132 of the Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community (2019/C 384 I/01).

1. Limitation to Out-of-Purpose Use and Provision of Personal Information (Articles 3, 15 and 18 of the Act)

<Personal Information Protection Act

(Act No. 16930, partially amended on February 4, 2020)>

Article 3 (Principles for Protecting Personal Information) (1) The personal information controller shall specify explicitly the purposes for which personal information is processed; and shall collect personal information lawfully and fairly to the minimum extent necessary for such purposes.

(2) The personal information controller shall process personal information in an appropriate manner necessary for the purposes for which the personal information is processed, and shall not use it beyond such purposes.

Article 15 (Collection and Use of Personal Information) (1) A personal information controller may collect personal information in any of the following circumstances, and use it with the scope of the purpose of collection:

1. Where consent is obtained from a data subject;
2. Where special provisions exist in laws or it is inevitable to observe legal obligations;
3. Where it is inevitable for a public institution's performance of its duties under its jurisdiction as prescribed by statutes, etc.;
4. Where it is inevitably necessary to execute and perform a contract with a data subject;
5. Where 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 his or her legal representative is not in a position to express intention, or prior consent cannot be obtained owing to unknown addresses, etc.;
6. Where it is necessary to attain the justifiable interest of a personal information controller, which such interest is manifestly superior to the rights of the data subject. In such cases, processing shall be allowed only to the extent the processing is substantially related to the justifiable interest of the personal information controller and does not go beyond a reasonable scope.

Article 18 (Limitation to Out-of-Purpose Use and Provision of Personal Information) (1) A personal information controller shall not use personal information beyond the scope provided for in Articles 15 (1) and 39-3 (1) and (2), or provide it to any third party beyond the scope provided for in Article 17 (1) and (3).

(2) Notwithstanding paragraph (1), where any of the following subparagraphs applies, a personal information controller may use personal information or provide it to a third party for other purposes, unless doing so is likely to unfairly infringe on the interest of a data subject or third party: Provided, That information and communications service providers [as set forth in Article 2 (1) 3 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.; hereinafter the same shall apply] processing the personal information of users [as set forth in Article 2 (1) 4 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.; hereinafter the same shall apply] are only subject to subparagraphs 1 and 2, and subparagraphs 5 through 9 are applicable only to public institutions:

1. Where additional consent is obtained from the data subject;

2. Where other special provisions in laws exist;

3. Where 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 his or her legal representative is not in a position to express intention, or prior consent cannot be obtained owing to unknown addresses;

4. Deleted;<by Act No. 16930, Feb. 4, 2020>

5. Where it is impossible to perform the duties under its jurisdiction as provided for in any Act, unless the personal information controller uses personal information for other purpose than the intended one, or provides it to a third party, and it is subject to the deliberation and resolution by the Commission;

6. Where it is necessary to provide personal information to a foreign government or international organization to perform a treaty or other international convention;

7. Where it is necessary for the investigation of a crime, indictment and prosecution;

8. Where it is necessary for a court to proceed with trial-related duties;

9. Where it is necessary for the enforcement of punishment, probation and custody.

omitted (3) ~ (4)

(5) Where a personal information controller provides personal information to a third party for other purpose than the intended one in any case provided for in paragraph (2), the personal information controller shall request the recipient of the personal information to limit the purpose and method of use and other necessary matters, or to prepare necessary safeguards to ensure the safety of the personal information. In such cases, the person in receipt of such request shall take necessary measures to ensure the safety of the personal information.

(i) Paragraphs 1 and 2 of Article 3 of the Act prescribe the principle that a personal information controller must collect only the minimum personal information necessary for performing the purpose of processing the personal information legally and lawfully, and should not use it for purposes other than the intended one.[3]

(ii) According to this principle, Paragraph 1 of Article 15 of the Act prescribes that when a personal information controller collects personal information, personal information may be used within the purpose of collection, and Paragraph 1 of Article 18 prescribes that personal information should not be used beyond the purpose of collection or provided to a third party.

(iii) Also, even if personal information may be used for purposes other than the intended one or provided to a third party in the exceptional cases[4] described in the subparagraphs of Paragraph 2 of Article 18 of the Act, it must be requested that the purpose or method of use should be restricted so that personal information can be processed safely according to Paragraph 5, or measures necessary for ensuring the safety of personal information should be taken.

[3] As these provisions set out general principles that apply to any processing of personal information, including where such processing is specifically regulated by other Acts, the clarifications in this section also apply where personal data is processed on the basis of other laws (see e.g. Article 15(1) of the Credit Information Act, which specifically refers to these provisions).

[4] Information communication service providers are only subject to Article 18(2) subparagraphs 1 and 2. Subparagraphs 5 through 9 are applicable only to public institutions.

(iv). The above provisions shall be applied equally to the processing of all personal information received within the area of Korea's legal jurisdiction from a third country, regardless of the nationality of the data subject.

(v). For instance, if a personal information controller in the EU transfers personal information to a Korean personal information controller according to the adequacy decision of the European Commission, the EU personal information controller's purpose of transferring the personal information shall be regarded as the Korean personal information controller's purpose of collecting personal information, and in such cases, the Korean personal information controller may only use the personal information or provide it to a third party within the purpose of collection except for the exceptional cases described in the subparagraphs of Paragraph 2 of Article 18 of the Act.

2. Limitation to Onward transfer of Personal data (Articles 17(3) (4), Article 18 of the Act)

<Personal Information Protection Act

(Act No. 16930, partially amended on February 4, 2020)>

Article 17 (Provision of Personal Information) (1) omit

(2) A personal information controller shall inform a data subject of the following matters when it obtains the consent under paragraph (1) 1. The same shall apply when any of the following is modified:

1. The recipient of personal information;
2. The purpose for which the recipient of personal information uses such information;
3. Particulars of personal information to be provided;
4. The period during which the recipient retains and uses personal information;
5. The fact that the data subject is entitled to deny consent, and disadvantages, if any, resulting from the denial of consent.

(3) A personal information controller shall inform a data subject of the matters provided for in paragraph (2), and obtain the consent from the data subject in order to provide personal information to a third party overseas; and shall not enter into a contract for the cross-border transfer of personal information in violation of this Act.

(4) A personal information controller may provide personal information without the consent of a data subject within the scope reasonably related to the purposes for which the personal information was initially collected, in accordance with the matters prescribed by Presidential Decree taking into consideration whether disadvantages are caused to the data subject, whether necessary measures to secure safety, such as encryption, have been taken, etc.

※ Please see pages 3, 4 and 5 for Article 18

< **Enforcement Decree of the Personal Information Protection Act**

([Enforcement Date 05. Feb, 2021.] [Presidential Decree No. 30892, 04.Aug, 2020., Amends Other Acts])>

Article 14-2 (Standards on Additional Use/Provision of Personal Information, etc.)

(1) If a personal information controller uses or provides personal information (hereinafter referred to as "additional use or provision of personal information") without the consent of

the data subject in accordance with Article 15 (3) of the Act or Article 17 (4) of the Act, the personal information controller shall consider the following matters:

1. Whether it is reasonably related to the original purpose for which the personal information was collected;

2. Whether additional use or provision of personal information is foreseeable in light of the circumstances under which the personal information was collected and processing practices;

3. Whether additional use or provision of personal information does not unfairly infringe on the interests of the data subject; and

4. Whether the measures required to ensure security such as pseudonymization or encryption have been taken.

(2) The personal information controller shall disclose in advance the criteria for assessing the matters referred to in the subparagraphs of paragraph (1) in the Privacy Policy under Article 30 (1) of the Act, and the privacy officer under Article 31 (1) of the Act shall check whether the personal information controller is using or providing additional personal information in accordance with the relevant standards.

(i) If the personal information controller provides personal information to a third party overseas, he/she must inform data subjects in advance of all the matters described in Article 17(2) of the Act and obtain their consent, except for cases falling under (1) or (2). No contract should be entered concerning cross-border provision of personal data in violation of this Act.

(1) If personal information is provided within the scope reasonably related to the initial purpose of collection according to Paragraph 4 of Article 17 of the Act. However, the cases to which this provision can be applied are limited to cases where the standards for additional use and provision of personal information, prescribed in Article 14-2 of the Enforcement Decree, are met. In addition, the personal information controller must consider whether the provision of personal information may cause disadvantages to data subjects, and whether he/she has taken necessary measures for securing safety, such as encryption.

(2) If personal information can be provided to a third party in exceptional cases mentioned in Paragraph 2 of Article 18 of the Act (see pages 3~5). However even in such cases, if the provision of such personal information is likely to unfairly infringe the interests of the data subject or a third party, personal information cannot be provided to a third party. Moreover, the provider of personal information must request the recipient of personal information to limit the purpose or method of using the personal information or take measures necessary for ensuring the safety thereof so that the personal information can be processed safely.

(ii) If personal information is provided to a third party overseas, it may not receive the level of protection guaranteed by the Personal Information Protection Act of Korea due to differences in personal information protection systems of different countries. Accordingly, such cases will be deemed as ‘cases where disadvantages may be caused to the data subject’ mentioned in Paragraph 4 of Article 17 of the Act or ‘cases where the interest of a data subject or third party is infringed unfairly’ mentioned in Paragraph 2 of Article 18 of the Act and Article 14-2 of the Enforcement Decree of the same Act.[5] To fulfil the requirements of

[5] Pursuant to Article 18(2) lit. 2, PIPA, this also applies when personal information is disclosed to third parties

these provisions, the personal information controller and third party must therefore explicitly ensure a level of protection equivalent to the Act, including the guarantee of the data subject's exercise of his/her rights in legally binding documents such as contracts, even after personal information is transferred overseas.

3. Notification for the data where personal data have not been obtained from the data subject (Article 20 of the Act)

<Personal Information Protection Act

(Act No. 16930, partially amended on February 4, 2020)>

Article 20 (Notification on Sources, etc. of Personal Information Collected from Third Parties) (1) When a personal information controller processes personal information collected from third parties, the personal information controller shall immediately notify the data subject of the following matters at the request of such data subject:

1. The source of collected personal information;

2. The purpose of processing personal information;

3. The fact that the data subject is entitled to demand suspension of processing of personal information, as prescribed in Article 37.

(2) Notwithstanding paragraph (1), when a personal information controller satisfying the criteria prescribed by Presidential Decree taking into account the types and amount of processed personal information, number of employees, amount of sales, etc., collects personal information from third parties and processes the same pursuant to Article 17 (1) 1, the personal information controller shall notify the data subject of the matters referred to in paragraph (1): Provided, That this shall not apply where the information collected by the personal information controller does not contain any personal information, such as contact information, through which notification can be given to the data subject.

(3) Necessary matters in relation to the time, method, and procedure of giving notification to the data subject pursuant to the main sentence of paragraph (2), shall be prescribed by Presidential Decree.

(4) Paragraph (1) and the main clause of paragraph (2) shall not apply to any of the following circumstances: Provided, That this shall be the case only where it is manifestly superior to the rights of data subjects under this Act:

1. Where personal information, which is subject to a notification request, is included in the personal information files referred to in any of the subparagraphs of Article 32 (2);

2. Where such notification is likely to cause harm to the life or body of any other person, or unfairly damages the property and other interests of any other person.

(i) If the personal information controller receives the personal information transferred from the EU based on its adequacy decision[6], he/she must notify the following information (1) through (5) to the data subject without undue delay, and in any event not later than one month from the transfer.

---

overseas on the basis of provisions in other Acts (such as e.g. the Credit Information Act).

[6] The obligations under (i), (ii) and (iii) equally apply when the controller that receives personal information from the EU on the basis of the adequacy decision processes such information on the basis of other Acts, such as e.g. the Credit Information Act.

(1) The name and contact information of the persons who transfer and receive the personal information.

(2) The items or categories of the personal information transferred.

(3) The purpose of collecting and using the personal information (as set by data exporter pursuant to point 1 of this Notification).

(4) The personal information retention period.

(5) Information on the data subject's rights in regard to the processing of the personal information, the method and procedure of exercising the rights and any disadvantages if the exercise thereof causes disadvantages.

(ii) Also, if the personal information controller provides the personal information in (i) to a third party in the Republic of Korea or abroad, he/she must notify the information (1) through (5) to the data subject before the personal information is provided.

(1) The name and contact information of the persons who provide and receive the personal information.

(2) The items or categories of the personal information provided.

(3) The country to which the personal information shall be provided, the envisaged date and method of providing it (limited to cases where personal information shall be provided to a third party overseas).

(4) The personal information provider's purpose and legal basis of providing the personal information

(5) Information on the data subject's rights in regard to the processing of personal information, the method and procedure of exercising the rights, and any disadvantages if the exercise thereof causes disadvantages.

(iii) The personal information controller may not apply (i) or (ii) in any of the following cases (1) through (4).

(1) If the personal information that needs to be notified is included in any of the following personal information files mentioned in Paragraph 2 of Article 32 of the Act, to the extent that the interests protected by this provision are manifestly superior to the rights of the data subject, and only as long as the notification would threaten the pursuit of the interests at stake, for instance jeopardizing ongoing criminal investigations or threatening national security.

(2) If and for as long as the notification is likely to harm the life or body of another person, or unfairly infringe on the property interests of another person, where those rights or interests are manifestly superior to the rights of the data subject.

(3) If the data subject already possesses the information that the personal information controller must notify according to (i) or (ii).

(4) If the personal information controller does not have any contact information of the data subject or it involves excessive efforts to contact the data subject, including in the context of processing under the conditions set out in Section 3 PIPA. In determining whether or not it is possible to contact the data subject, or whether this involves excessive efforts, the possibility to cooperate with the data exporter in the EU should be taken into account.

4. Scope of application of the special exemption to the processing of

pseudonymised information (Articles 28-2, 28-3, 28-4, 28-5, 28-6 and 28-7, Article 3 and Article 58-2 of the Act)

<Personal Information Protection Act

(Act No. 16930, partially amended on February 4, 2020)>

Chapter III Processing of Personal Information

SECTION 3 Special Cases concerning Pseudonymous Data

Article 28-2 (Processing of Pseudonymous Data) (1) A personal information controller may process pseudonymized information without the consent of data subjects for statistical purposes, scientific research purposes, and archiving purposes in the public interest, etc.

(2) A personal information controller shall not include information that may be used to identify a certain individual when providing pseudonymized information to a third party according to paragraph (1).

Article 28-3 (Restriction on Combination of Pseudonymous Data) (1) Notwithstanding Article 28-2, the combination of pseudonymized information processed by different personal information controllers for statistical purposes, scientific research and preservation of records for public interest, etc. shall be conducted by a specialized institution designated by the Protection Commission or the head of the related central administrative agency.

(2) A personal information controller who intends to release the combined information outside the organization that combined the information shall obtain approval from the head of the specialized institution after processing the information into pseudonymized information or the form referred to in Article 58-2.

(3) Necessary matters including the procedures and methods of combination pursuant to paragraph (1), standards and procedures to designate, or cancel the designation of, a specialized institution management and supervision, and standards and procedures of exporting and approval pursuant to paragraph (2) shall be prescribed by Presidential Decree.

Article 28-4 (Obligation to Take Safety Measures for Pseudonymous Data) (1) When processing the pseudonymized information, a personal information controller shall take such technical, organizational and physical measures as separately storing and managing additional information needed for restoration to the original state, as may be necessary to ensure safety as prescribed by Presidential Decree so that the personal information may not be lost, stolen, divulged, forged, altered, or damaged.

(2) A personal information controller who intends to process the pseudonymized information shall prepare and keep records relating to matters prescribed by the Presidential Decree including the purpose of processing the pseudonymized information, and a third party recipient when pseudonymized information is provided, to manage the processing of pseudonymized information.

Article 28-5 (Prohibited Acts for the Processing of the Pseudonymized Information) (1) No one shall process the pseudonymized information for the purpose of identifying a certain individual.

(2) When information identifying a certain individual is generated while the pseudonymized information is processed, the personal information controller shall cease the processing of the information, and retrieve and destroy the information immediately.

Article 28-6 (Imposition of Administrative Surcharges for the Processing of the Pseudonymized Information) (1) The Commission may impose a fine equivalent to less than three-hundredths of total sales on data controller who has processed data for the purpose of identifying a specific individual in violation of Article 28-5 (1): Provided, That in case where there is no sales or difficulty in calculating the sales revenues, the data controller may be subject to a fine of not more than 400 million won or three-hundredths of the capital amount, whichever is greater.

(2) Article 34-2 (3) through (5) shall apply mutatis mutandis to matters necessary to impose and collect administrative surcharges.

Article 28-7 (Scope of Application) @Articles 20, 21, 27, 34 (1), 35 through 37, 39-3, 39-4, 39-6 through 39-8 shall not apply to the pseudonymized information.

Chapter I General Provisions

Article 3 (Principles for Protecting Personal Information) (1) The personal information controller shall specify explicitly the purposes for which personal information is processed; and shall collect personal information lawfully and fairly to the minimum extent necessary for such purposes.

(2) The personal information controller shall process personal information in an appropriate manner necessary for the purposes for which the personal information is processed, and shall not use it beyond such purposes.

(3) The personal information controller shall ensure personal information is accurate, complete, and up to date to the extent necessary in relation to the purposes for which the personal information is processed.

(4) The personal information controller shall manage personal information safely according to the processing methods, types, etc. of personal information, taking into account the possibility of infringement on the data subject's rights and the severity of the relevant risks.

(5) The personal information controller shall make public its privacy policy and other matters related to personal information processing; and shall guarantee the data subject's rights, such as the right to access their personal information.

(6) The personal information controller shall process personal information in a manner to minimize the possibility of infringing the privacy of a data subject.

(7) If it is still possible to fulfil the purposes of collecting personal information by processing anonymized or pseudonymised personal information, the personal information controller shall endeavor to process personal information through anonymization, where anonymization is possible, or through pseudonymisation, if it is impossible to fulfil the purposes of collecting personal information through anonymization

(8) The personal information controller shall endeavor to obtain trust of data subjects by observing and performing such duties and responsibilities as provided for in this Act and other related statutes.

Chapter IX Supplementary Provisions

Article 58-2 (Exemption from Application) This Act shall not apply to information that no longer identifies a certain individual when combined with other information, reasonably considering time, cost, technology, etc. <This Article Newly Inserted by Act No. 16930, Feb. 4, 2020>

(i) Chapter III, Section 3 Special Cases concerning Pseudonymous Data (Art. 28-2 to Art.28-7) allows the processing of pseudonymised information without the consent of the data subject for the purpose of compiling statistics, scientific research, preservation of public records, etc. (Article 28-2), but in such cases, appropriate safeguards and prohibitions necessary for protecting the rights of data subjects are mandatory (Articles 28-4 and 28-5), penalty surcharges may be imposed on violators (Article 28-6) and certain safeguards otherwise available under PIPA do not apply (Article 28-7).

(ii) These provisions shall not apply to cases where pseudonymised information is processed for purposes other than compiling statistics, scientific research, preservation of public records, etc. For instance, if the personal information of an EU individual, which was transferred to Korea according to the adequacy decision of the European Commission, is pseudonymised for purposes other than compiling statistics, scientific research, preservation of public records, etc., the special provisions in Chapter III, Section 3 shall not apply.[7]

(iii) Where a personal information controller processes pseudonymised information for the purpose of compiling statistics, scientific research, preservation of public records, etc. and if the pseudonymised information has not be destroyed once the specific purpose of processing has been fulfilled in line with Article 37 of the Constitution and Article 3 (Principles for Protecting Personal Information) of the Act, it shall anonymise the information with a view to ensure that it no longer identifies a specific individual, alone or when combined with other information, reasonably considering time, cost, technology, etc., in accordance with Article 58-2 PIPA.

5. Corrective measures, etc. (Paragraphs 1, 2 and 4 of Article 64 of the Act)

<Personal Information Protection Act

(Act No. 16930, partially amended on February 4, 2020)>

Article 64 (Corrective Measures) (1) Where the Protection Commission deems that there is substantial ground to deem that there has been infringement with respect to personal information, and failure to take action is likely to cause damage that is difficult to remedy, it may order the violator of this Act (excluding central administrative agencies, local governments, the National Assembly, the Court, the Constitutional Court, and the National Election Commission) to take any of the following measures:

1. To suspend infringement with respect to personal information;

2. To temporarily suspend personal information processing;

3. Other measures necessary to protect personal information and to prevent personal information infringement.

(2) Where the head of a related central administrative agency deems that there is substantial ground to deem that there has been an infringement of personal information, and failure to take action is likely to cause damage that is difficult to remedy, he or she may order a personal information controller to take any of the measures provided for in paragraph (1) pursuant to the statutes under such related central administrative agency's jurisdiction.

(4) When a central administrative agency, a local government, the National Assembly, the Court, the Constitutional Court, or the National Election Commission violates this Act, the Protection Commission may recommend the head of the relevant agency to take any of the measures provided for in paragraph (1).

[7] Similarly, the exception of Article 40-3 of the Credit Information Act only applies to the processing of pseudonymised credit information for purposes of compiling statistics, scientific research and the preservation of public records.

In such cases, upon receiving the recommendation, the agency shall comply therewith unless there are extraordinary circumstances.

(i) First, court precedents[8] [9] interpret 'damage that is difficult to remedy' as a case that could cause damage to an individual's personal rights or privacy.

(ii) Accordingly, 'substantial ground to deem that there has been an infringement with respect to personal information, and failure to take action is likely to cause damage that is difficult to remedy' prescribed in Paragraphs 1 and 2 of Article 64, refer to cases where a violation of the law is deemed to be likely to infringe on the rights and freedom of individuals in regard to personal information. This will be applicable whenever any of the principles, rights and duties, included in the law to protect personal information, are violated.[10]

(iii) According to Paragraph 4 of Article 64 of the Personal Information Protection Act is a measure in regard to 'a violation of this Act,' i.e. action against an infringement of PIPA.

A central administrative agency, etc., as a public authority bound to the rule of law, may not violate any law and is obligated to take a corrective measure, including to immediately stop the action, and compensate for damages in the exceptional case where an illegal act was nevertheless committed.

Accordingly, even without any intervention by the Protection Commission according to Paragraph 4 of Article 64 of PIPA, a central administrative agency etc. must take a corrective measure against violations if it becomes aware of any violation of the law.

In particular, where the Protection Commission has recommended a corrective measure, it will normally be objectively clear to the central administrative agency, etc. that it has violated the law. Thus, in order to justify why it considers that a recommendation by the Protection Commission should not be followed, a central administrative agency, etc. must present clear grounds that can prove that it did not violate the law. The recommendation must be followed unless the Protection Commission determines that this is indeed not the case.

In consideration of this, the 'extraordinary circumstances' in Paragraph 4 of Article 64 of the Personal Information Protection Act must be strictly limited to extraordinary circumstances in which there are clear grounds for central administrative agencies etc. to prove that 'this Act was in fact not violated,' such as 'cases where there are extraordinary (factual or legal) circumstances' that the Protection Commission did not know when making its recommendation initially and the Protection Commission determines that indeed no violation has occurred.

6. Application of PIPA to the processing of personal data for national security purposes including investigation of infringements and enforcement in accordance PIPA(Article 7-8, Article 7-9, Article 58, Article 3, Article 4 and Article 62 of PIPA)

<Personal Information Protection Act

(Act No. 16930, partially amended on February 4, 2020)>

8 (Supreme Court Judgement 97Da10215,10222 dated January 26, 1999) If the criminal facts of the accused are disclosed through the media, it is likely to cause irreparable mental and physical damage to not only the victim, i.e. the plaintiff, but also people around him/her, including families.

9 (Seoul High Court Judgment 2006Na92006 dated January 16, 2008) If a defamatory article is published, it is likely to cause serious irreparable damage to the person involved.

10 The same principles as set out in point (ii) apply to Article 45-4 of the Credit Information Act.

Article 7-8 (Work of the Protection Commission) (1) The Protection Commission shall perform the following work: […]

3. Matters concerning investigation into infringement upon the right of data subjects and the ensuing dispositions;

4. Handling of complaints or remedial procedures relating to personal information processing and mediation of disputes over personal information;

[…]

Article 7-9 (Matters Subject to Deliberation and Resolution by the Protection Commission) (1) The Protection Commission shall deliberate and resolve on the following matters: […]

5. Matters concerning the interpretation and operation of law related to the protection of personal information;

[…]

Article 58 (Partial Exclusion of Application) (1) Chapter III through VII shall not apply to any of the following personal information:

1. Personal information collected pursuant to the Statistics Act for processing by public institutions;

2. Personal information collected or requested to be provided for the analysis of information related to national security;

3. Personal information processed temporarily where it is urgently necessary for the public safety and security, public health, etc.;

4. Personal information collected or used for its own purposes of reporting by the press, missionary activities by religious organizations, and nomination of candidates by political parties, respectively.

[omitted (2) and (3)]

(4) In the case of processing personal information pursuant to paragraph (1), a personal information controller shall process the personal information to the minimum extent necessary to attain the intended purpose for the minimum period; and shall also make necessary arrangements, such as technical, managerial and physical safeguards, individual grievance handling and other necessary measures for the safe management and appropriate processing of such personal information.

Article 3 (Principles for Protecting Personal Information) (1) The personal information controller shall specify explicitly the purposes for which personal information is processed; and shall collect personal information lawfully and fairly to the minimum extent necessary for such purposes.

(2) The personal information controller shall process personal information in an appropriate manner necessary for the purposes for which the personal information is processed, and shall not use it beyond such purposes.

(3) The personal information controller shall ensure personal information is accurate, complete, and up to date to the extent necessary in relation to the purposes for which the personal information is processed.

(4) The personal information controller shall manage personal information safely according to the processing methods, types, etc. of personal information, taking into account the

possibility of infringement on the data subject's rights and the severity of the relevant risks.

(5) The personal information controller shall make public its privacy policy and other matters related to personal information processing; and shall guarantee the data subject's rights, such as the right to access their personal information.

(6) The personal information controller shall process personal information in a manner to minimize the possibility of infringing the privacy of a data subject.

(7) If it is still possible to fulfil the purposes of collecting personal information by processing anonymized or pseudonymised personal information, the personal information controller shall endeavor to process personal information through anonymization, where anonymization is possible, or through pseudonymisation, if it is impossible to fulfil the purposes of collecting personal information through anonymization.

(8) The personal information controller shall endeavor to obtain trust of data subjects by observing and performing such duties and responsibilities as provided for in this Act and other related statutes.

Article 4 (Rights of Data Subjects) A data subject has the following rights in relation to the processing of his or her own personal information:

1. The right to be informed of the processing of such personal information;

2. The right to determine whether or not to consent and the scope of consent regarding the processing of such personal information;

3. 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;

4. The right to suspend the processing of, and to request correction, deletion, and destruction of such personal information;

5. The right to appropriate redress for any damage arising out of the processing of such personal information through a prompt and fair procedure.

Article 62 (Reporting on Infringements) (1) Anyone who suffers infringement of rights or interests relating to his or her personal information in the course of personal information processing by a personal information controller may report such infringement to the Protection Commission.

(2) The Protection Commission may designate a specialized institution in order to efficiently receive and handle the claim reports pursuant to paragraph (1), as prescribed by Presidential Decree. In such cases, such specialized institution shall establish and operate a personal information infringement call centre (hereinafter referred to as the "Privacy Call Centre").

(3) The Privacy Call Center shall perform the following duties:

1. To receive claim reports and provide consultation in relation to personal information processing;

2. To investigate and confirm incidents and hear opinions of related parties;

3. Duties incidental to subparagraphs 1 and 2.

(4) The Protection Commission may, if necessary, dispatch its public official to the specialized institution designated under paragraph (2) pursuant to Article 32-4 of the State Public Officials Act in order to efficiently investigate and confirm the incidents pursuant to

paragraph (3) 2

(i) The collection of personal information for national security purposes is regulated by specific laws that empower competent authorities (e.g. the National Intelligence Service) to intercept communications or request disclosure under certain conditions and safeguards (hereafter: "national security laws"). These national security laws include, for instance, the Communications Privacy Protection Act, the Act on Anti-Terrorism for the Protection of Citizens and Public Security or the Telecommunications Business Act. In addition, the collection and further processing of personal information has to comply with the requirements of PIPA. In this regard, Article 58(1) lit. 2 PIPA provides that Chapters III through VII shall not apply to personal information collected or requested to be provided for the analysis of information related to national security. This partial exception therefore applies to the processing of personal information for national security purposes.

At the same time, Chapter I (General provisions), Chapter II (Establishment of personal information protection policies, etc.), Chapter VIII (Class-action lawsuit over data infringement), Chapter IX (Supplementary provisions) and Chapter X (Penalty provisions) of PIPA apply to the processing of such personal information. This includes the general data protection principles set out in Article 3 (Principles of protecting personal information) and the individual rights guaranteed by Article 4 PIPA (Rights of data subjects).

In addition, Article 58(4) PIPA provides that such information must be processed to the minimum extent necessary to attain the intended purpose and for the minimum period; in addition, it requires the personal information controller to put in place the necessary measures to ensure safe data management and appropriate processing, such as technical, managerial and physical safeguards, as well as measures for the appropriate handling of individual grievances.

Finally, the provisions governing the tasks and powers of the PIPC (including Article 60-65 PIPA on the handling of complaints and the adoption of recommendations and corrective measures) as well as the provisions on administrative and criminal penalties (Article 70 et seq. PIPA) apply. According to Article 7-8(1)3,4 and Article 7-9(1)5 PIPA, these investigatory and corrective powers, including when exercised in the context of handling complaints, also cover possible infringements of the rules contained in specific laws setting out the limitations and safeguards with respect to the collection of personal information, such as the national security laws. Given the requirements in Article 3(1) PIPA for the lawful and fair collection of personal information, and such infringement constitutes a violation of "this Act" within the meaning of Articles 63 and 64, allowing the PIPC to carry out an investigation and to take corrective measures.[11] The exercise of these powers by the PIPC supplements, but does not replace, the powers of the National Human Rights Commission under the Human Rights Commission Act.

The application of the core principles, rights and obligations of PIPA to the processing of personal information for national security purposes reflects the guarantees enshrined in the Constitution for the protection of the individual's right to control his or her own personal information. As recognised by the Constitutional Court, this includes the right of an individual[12] "to personally decide when, to whom or by whom, and to what extent his or her information will be disclosed or used. It is a basic right[13], […], existing to protect the

[11] As regards corrective measures pursuant to Article 64, see also Section 5 above.
[12] Constitutional Court Judgment, 99HunMa513, 2004HunMa190, dated May 26, 2005
[13] Constitutional Court Judgment, 2003HunMa282, dated July 21, 2005

personal freedom of decision from the risk caused by the enlargement of state functions and info-communication technology". Any restriction to that right, for example when necessary for the protection of national security, requires a balancing of the rights and interests of the individual against the relevant public interest and may not affect the essence of the right (Article 37(2) of the Constitution).

Therefore, when processing personal information for national security purposes, the controller (e.g. NIS) shall, inter alia:

(1) Specify explicitly the purposes for which personal information is processed and collect personal information lawfully and fairly to the minimum extent necessary for such purposes (Article 3(1) PIPA); specifically, it shall only collect and further process the personal information for the purpose of performing duties under the relevant statutes such as the National Intelligence Service Act;

(2) Process personal information to the minimum extent, and for the minimum period, necessary to attain the intended purpose (Article 58(4) PIPA); upon attainment of the purpose of processing, the controller shall irreversibly destroy the personal information, unless further retention is specifically mandated by statute, in which case the relevant personal information shall be stored and managed separately from other personal information, not be used for any purpose other than that specified in the statute and destroyed upon the end of the retention period;

(3) Process personal information in an appropriate manner necessary for the purposes for which the personal information is processed, and shall not use it beyond such purposes (Article 3(2) PIPA);

(4) Ensure that personal information is accurate, complete and up to date to the extent necessary in relation to the purposes for which the personal information is processed (Article 3(3) PIPA);

(5) Manage personal information safely according to the processing methods, types, etc. of personal information, taking into account the possibility of infringements of the data subject's rights and the severity of the relevant risks (Article 3(4) PIPA);

(6) Make public its privacy policy and other matters related to personal information processing (Article 3(5) PIPA);

(7) Process personal information in a manner such as to minimise the possibility of infringing the privacy of a data subject (Article 3(6) PIPA).

(ii) In accordance with Article 58(4) PIPA, the controller (e.g. authorities competent for national security such as the NIS) shall make the necessary arrangements, such as putting in place technical, managerial and physical safeguards, to ensure compliance with these principles and the appropriate processing of personal information. This may for instance include specific measures to ensure the safety of personal information, such as restrictions on access to personal information, access controls, logs, providing employees with dedicated training on the handling of personal information, etc.

In addition, in accordance with Articles 3(5) and 4 PIPA, data subjects shall, inter alia, have the following rights with respect to personal information processed for national security purposes:

(1) The right to obtain confirmation as to whether or not his or her personal information is being processed as well as information about the processing, and to access that information, including the provision of copies (Article 4(1), (3) PIPA);

(2) The right to suspend processing, and to the correction, deletion and destruction, of personal information (Article 4(4) PIPA).

(iii) A data subject may file a request in the exercise of these rights directly with the controller or indirectly via the Protection Commission, and may authorise his or her representative to do so. Where the data subject files a request, the controller shall grant the right without delay; provided, however, that it may delay, limit or deny the right if specifically provided for or inevitable to comply with other statutes to the extent and for as long as necessary and proportionate to protect an important objective of public interest (for instance to the extent that and for as long as granting the right would jeopardise an ongoing investigation or threaten national security), or where granting the right may cause damage to the life or body of a third party, or unjustified infringement of property and other interests of a third party. Where the request is denied or restricted, it shall notify the data subject of the reasons without delay. The controller shall prepare the method and procedure to enable data subjects to file requests and publicly announce them so that data subjects may become aware of them.

Moreover, in accordance with Article 58(4) PIPA (requirement to ensure the appropriate handling of individual grievances) and Article 4(5) PIPA (the right to appropriate redress for any damage arising out of the processing of personal information, through a prompt and fair procedure), data subjects shall have the right to obtain redress. This includes the right to report an alleged violation to the Personal Information Infringement Report Center (in accordance with Article 62(3) PIPA), file a complaint with the PIPC pursuant to Article 62 PIPA about any violation with respect to rights or interests relating to an individual's personal information and to obtain judicial redress against decisions or inaction of the PIPC under the Administrative Litigation Act. In addition, data subjects may obtain judicial redress under the Administrative Litigation Act if there has been an infringement upon their rights or interests due to a disposition or omission by the controller (e.g. unlawful collection of personal data), or obtain compensation for damages in accordance with the State Compensation Act. These redress avenues are available both in case of possible infringements of the rules contained in specific laws setting out the limitations and safeguards with respect to the collection of personal information, such as the national security laws, and of PIPA.

An individual from EU may submit a complaint to the PIPC through his/her national data protection authority, and PIPC will notify the individual through the national data protection authority, after the investigation and corrective measure (if applicable) is concluded.

ANNEX II

May 18, 2021

His Excellency Mr. Didier Reynders, Commissioner for Justice of the European Commission

Your Excellency,

I welcome the constructive discussions between Korea and the European Commission aiming at building the framework for transfer of personal data from EU to Korea.

Upon the request from the European Commission to the government of Korea, I am sending a document attached herewith providing an overview of the legal framework concerning access to information by the government of Korea.

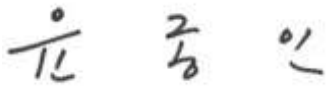
This document concerns many ministries and agencies of the government of Korea, and regarding the contents of the document, the relevant ministries and agencies (Personal Information Protection Commission, Ministry of Justice, National Intelligence Service, National Human Rights Commission of Korea, National Counter Terrorism Center, Korea Financial Intelligence Unit) are responsible for the passages within the scope of their respective competences. Please find below the relevant ministries and agencies and respective signatures.

The Personal Information Protection Commission accepts all inquiries on this document and will coordinate the necessary responses among the relevant ministries and agencies.

I hope that this document would be helpful in making decisions at the European Commission.

I do appreciate your great contribution to date in this matter.

Sincerely yours,



Yoon Jong In
Chairperson of Personal Information Protection Commission

This Document was drawn up by Personal Information Protection Commission and the following ministries and agencies concerned.

Park Jie Won
President(Director), National Intelligence Service

Lee Jung Soo
Director General, Ministry of Justice

Choi Young Ae
Chairperson, National Human Rights Commission of Korea

Kim Hyuck Soo
Director, National Counter Terrorism Center

Kim, Jeong Kag
Commissioner, Korea Financial Intelligence Unit

Legal framework for the collection and use of personal data by Korean public authorities for law enforcement and national security purposes

The following document provides an overview of the legal framework for the collection and use of personal data by Korean public authorities for criminal law enforcement and national security purposes (hereinafter referred to as "*government access*"), in particular as regards the available legal bases, applicable conditions (limitations) and safeguards, as well as independent oversight and individual redress possibilities.

1. GENERAL LEGAL PRINCIPLES RELEVANT FOR GOVERNMENT ACCESS

1.1. Constitutional framework

The Constitution of the Republic of Korea lays down the right to privacy in general (Article 17) and the right to privacy of correspondence in particular (Article 18). It is the duty of the State to guarantee these fundamental rights.[14] The Constitution furthermore stipulates that the rights and freedoms of citizens may only be restricted by law and when necessary for national security, or the maintenance of law and order for public welfare.[15] Even when such restrictions are imposed, they may not affect the essence of the freedom or right.[16] The Korean courts have applied these provisions in cases concerning government interference with privacy. For example, the Supreme Court found that the monitoring of civilians violated the fundamental right to privacy, stressing that citizens have "*the right to self-determination of personal information.*"[17] In another case, the Constitutional Court held that privacy is a fundamental right that provides protection from state intervention and observation in the private life of citizens.[18]

The Korean Constitution furthermore guarantees that no person shall be arrested, detained, searched, interrogated, or items seized except as provided by law.[19] Moreover, searches and seizures may only be conducted on the basis of a warrant issued by a judge, upon request of a prosecutor, and in respect of due process.[20] In exceptional circumstances, i.e. where a criminal suspect is apprehended while committing a crime (*flagrante delicto*), or where there is a risk that a person suspected of committing a crime punishable by imprisonment of three years or more may escape or destroy evidence, investigative authorities may conduct a warrantless search or seizure, in which case they must request a warrant ex post.[21] These general principles are further developed in specific laws dealing with criminal procedure and the protection of communications (see below for a detailed overview).

With respect to foreign nationals, the Constitution stipulates that their status is guaranteed as prescribed by international law and treaties.[22] Several international agreements to which Korea is a party guarantee privacy rights, such as the International Covenant on Civil and

---

[14] Article 10 of the Constitution of the Republic of Korea, promulgated on 17 July 1948 (hereafter "the Constitution").

[15] Article 37(2) of the Constitution.

[16] Article 37(2) of the Constitution.

[17] Supreme Court of Korea Decision No. 96DA42789, 24 July 1998.

[18] Constitutional Court Decision No. 2002Hun-Ma51, 30 October 2003. Similarly, in Decision 99Hun-Ma513 and 2004Hun-Ma190 (consolidated), 26 May 2005, the Constitutional Court clarified that "*the right to control one's own personal information is a right of the subject of the information to personally decide when, to whom or by whom, and to what extent his or her information will be disclosed or used. It is a basic right, although not specified in the Constitution, existing to protect the personal freedom of decision from the risk caused by the enlargement of state functions and info-communication technology*."

[19] Article 12(1), first sentence of the Constitution.

[20] Article 16 and 12(3) of the Constitution.

[21] Article 12(3) of the Constitution.

[22] Article 6(2) of the Constitution.

Political Rights (Article 17), the Convention on the Rights of Persons with Disabilities (Article 22) and the Convention on the Rights of the Child (Article 16). In addition, while the Constitution in principle refers to the rights of "*citizens*", the Constitutional Court has ruled that also foreign nationals hold basic rights.[23] In particular, the Court held that the protection of dignity and a person's value as a human being as well as the right to seek happiness are rights of any human being, and not just of citizens.[24] The Court also clarified that the right to control one's information is considered to be a basic right, grounded in the right to dignity and the pursuit of happiness and the right to private life.[25] Although case law has so far not specifically dealt with the right to privacy of non-Korean nationals, it is therefore widely accepted among scholars that Articles 12-22 of the Constitution (which include the right to privacy as well as personal liberty) set out "*rights of human beings*."

Finally, the Constitution also provides for a right to claim just compensation from public authorities.[26] Moreover, on the basis of the Constitutional Court Act, any person whose fundamental rights guaranteed by the Constitution are infringed by the exercise of governmental power (excluding judgments of the courts) may lodge a constitutional complaint with the Constitutional Court.[27]

1.2. General data protection rules

The general data protection law in the Republic of Korea, the Personal Information Protection Act (hereafter "*PIPA*"), applies to both the private and public sector. With respect to public authorities, PIPA specifically refers to the obligation to formulate policies to prevent "*abuse and misuse of personal information, indiscrete surveillance and tracking, etc. and to enhance the dignity of human beings and individual privacy*."[28]

The processing of personal data for law enforcement purposes is subject to the entirety of PIPA's requirements. This means for instance that criminal law enforcement authorities must comply with the obligations for lawful processing, i.e. rely on one of the legal bases listed in PIPA for the collection, use or provision of personal information (Articles 15-18 PIPA), as well as the principles of purpose limitation (Article 3(1), (2) PIPA), proportionality/data minimisation (Article 3(1), (6) PIPA), limited data retention (Article 21 PIPA), data security, including data breach notification (Articles 3(4), 29 and 34 PIPA), and transparency (Articles 3(1), (5), 20, 30 and 32 PIPA). Specific safeguards apply with respect to sensitive information (Article 23 PIPA). Moreover, in accordance with Articles 3(5) and 4 PIPA, as well as Articles 35 to 39-2 PIPA, individuals can exercise their rights of access, correction, deletion and suspension vis-à-vis law enforcement authorities.

While PIPA therefore fully applies to the processing of personal data for criminal law enforcement purposes, it contains an exception when personal data is processed for national security purposes. According to Article 58(1) lit. 2 PIPA, Articles 15-50 PIPA do not apply to personal information collected or requested for the analysis of information related to national

---

[23] Constitutional Court Decision No. 93Hun-MA120, 29 December 1994. See also for example Constitutional Court Decision No. 2014Hun-Ma346 (31 May 2018), where the Court found that the constitutional right of a Sudanese national held at the airport to receive assistance of legal counsel was violated. In another case, the Constitutional Court found that the freedom to choose one's legal workplace is closely related to the right to pursue happiness as well as human dignity and value, and is therefore not reserved to citizens only but may also be guaranteed to foreigners that are legally employed in the Republic of Korea (Constitutional Court Decision No. 2007Hun-Ma1083, 29 September 2011).

[24] Constitutional Court Decision No. 99HeonMa494, 29 November 2001.

[25] See for instance Constitutional Court Decision No. 99HunMa513.

[26] Article 29(1) of the Constitution.

[27] Article 68(1) Constitutional Court Act.

[28] Article 5(1) PIPA.

security.[29] Conversely, Chapter I (General provisions), Chapter II (Establishment of personal information protection policies, etc.), Chapter VIII (Class-action lawsuit over data infringement), Chapter IX (Supplementary provisions) and Chapter X (Penalty provisions) of PIPA remain applicable. This includes the general data protection principles set out in Article 3 (Principles of protecting personal information) and the individual rights guaranteed by Article 4 PIPA (Rights of data subjects). This means that the main principles and rights are guaranteed also in this area. In addition, Article 58(4) PIPA provides that such information must be processed to the minimum extent necessary to attain the intended purpose and for the minimum period; it also requires the personal information controller to put in place the necessary measures to ensure safe data management and appropriate processing, such as technical, managerial and physical safeguards, as well as measures for the appropriate handling of individual grievances.

In Notification No. 2021-1 on Supplementary rules for the interpretation and application of the Personal Information Protection Act, the Personal Information Protection Commission (hereafter "*PIPC*") has further clarified how PIPA applies to the processing of personal data for national security purposes, in light of this partial exemption.[30] This includes in particular the rights of individuals (access, rectification, suspension and deletion) and the grounds as well as limitations for possible restrictions thereof. According to the Notification, the application of the core principles, rights and obligations of PIPA to the processing of personal data for national security purposes reflects the guarantees provided by the Constitution for the protection of the individual's right to control his or her own personal information. Any restriction to that right, for example when necessary for the protection of national security, requires a balancing of the rights and interests of the individual against the relevant public interest and may not affect the essence of the right (Article 37(2) of the Constitution).

2. GOVERNMENT ACCESS FOR LAW ENFORCEMENT PURPOSES

2.1. Competent public authorities in the area of law enforcement

Based on the Criminal Procedure Act (hereafter "*CPA*"), the Communications Privacy Protection Act (hereafter "*CPPA*") and the Telecommunications Business Act (hereafter "*TBA*"), the police, prosecutors and courts may collect personal data for criminal law enforcement purposes. To the extent the National Intelligence Service Act confers this power also onto the National Intelligence Service (hereafter "*NIS*"), it has to comply with the aforementioned Acts.[31] Finally, the Act on Reporting and Using Specified Financial Transaction Information (hereafter "ARUSFTI") provides a legal basis for financial institutions to disclose information to the Korea Financial Intelligence Unit (hereafter "KOFIU") for the purpose of preventing money laundering and terrorism financing. This specialised agency may in turn provide such information to law enforcement authorities. However, these disclosure obligations only apply to data controllers that process personal credit information pursuant to the Credit Information Act and are subject to the oversight of the Financial Services Commission. Since the processing of personal credit information by such controllers is excluded from the scope of the adequacy decision, the limitations and

[29] Article 58(1) lit. 2 PIPA.

[30] Notification No. 2021-1 of the PIPC on Supplementary rules for the interpretation and application of the Personal Information Protection Act, Section III, 6.

[31] See Article 3 NIS Act (Act No. 12948), which refers to criminal investigations of certain crimes, such as insurrection, rebellion and crimes related to national security (e.g. espionage). The procedures of the CPA regarding searches and seizures would apply in such a context, while the CPPA would govern the collection of communication data (see part 3 on the provisions dealing with access to communications for national security purposes).

safeguards that apply under the ARUSFTI are not described in further detail in this document.

2.2. Legal bases and limitations

The CPA (see 2.2.1), CPPA (see 2.2.2) and Telecommunications Business Act (see 2.2.3) provide legal bases for the collection of personal information for law enforcement purposes and set out the applicable limitations and safeguards.

2.2.1. Searches and seizures

2.2.1.1. Legal basis

Prosecutors and senior judicial police officers may only inspect articles, search persons or seize articles (1) if a person is suspected of having committed a crime (a criminal suspect), (2) it is necessary for the investigation and (3) the articles to be inspected, persons to be searched, and any articles seized are deemed to be connected with the case.[32] Likewise, courts may conduct searches and seize any articles to be used as evidence or liable to confiscation, as long as such articles or persons are considered to be connected with a specific case.[33]

2.2.1.2. Limitations and safeguards

As a general obligation, prosecutors and judicial police officers must respect the human rights of the criminal suspect as well as those of any other person concerned.[34] In addition, compulsory measures to achieve the purpose of the investigation may only be taken where explicitly provided for in the CPA and to the least extent necessary.[35]

Searches, inspections or seizures by police officers or prosecutors as part of a criminal investigation may only take place on the basis of a court-issued warrant.[36] The authority requesting a warrant must submit materials demonstrating the grounds for suspecting an individual of having committed a crime, that the search, inspection or seizure is necessary, and that the relevant articles to be seized exist.[37] As for the warrant, it must amongst other elements contain the names of the criminal suspect and the offence; the place, person or articles to be searched, or articles to be seized; the date of issuing; and the effective period of application.[38] Similarly, when, as part of ongoing Court proceedings, searches and seizures are carried out other than in open court, a court-issued warrant must be obtained beforehand.[39] The concerned individual and his/her defence council is notified in advance of the search or seizure and may be present when the warrant is being executed.[40]

When conducting searches or seizures and where the article to be searched is a computer disc or other data storage medium, in principle only the data itself (copied or printed out) will be seized rather than the entire medium.[41] The data storage medium itself may only be seized when it is considered substantially impossible to print out or copy the required data separately, or when it is considered substantially impracticable to otherwise accomplish the

[32] Article 215(1) and (2) CPA.
[33] Articles 106(1), 107 and 109 CPA.
[34] Article 198(2) CPA.
[35] Article 199(1) CPA.
[36] Article 215(1) and (2) CPA.
[37] Article 108(1) Regulation on Criminal Procedure.
[38] Article 114(1) CPA in conjunction with Article 219 CPA.
[39] Article 113 CPA.
[40] Article 121 and 122 CPA.
[41] Article 106(3) CPA.

purpose of the search.[42] The concerned individual must be notified of the seizure without delay.[43] There are no exceptions to this notification requirement under the CPA.

Warrantless searches, inspections and seizures may only take place in limited situations. First, this is the case when it is impossible to obtain a warrant because of urgency at the scene of an offence.[44] However, a warrant must subsequently be obtained without delay.[45] Second, warrantless searches and inspections may take place in loco when a criminal suspect is arrested or detained.[46] Finally, a prosecutor or senior judicial police officer may seize an article without a warrant when the article has been discarded by a criminal suspect or third person, or was voluntarily produced.[47]

Evidence that has been obtained in violation of the CPA will be considered inadmissible.[48] Moreover, the Criminal Act stipulates that illegal searches of persons or a person's place of residence, guarded building, structure, automobile, ship, aircraft or occupied room, is punishable by imprisonment for a maximum of three years.[49] This provision therefore also applies where objects, such as data storage devices, are seized during an illegal search.

2.2.2. Collection of communication information

2.2.2.1. Legal basis

The collection of communication information is governed by a specific Act, the CPPA. In particular, the CPPA stipulates a prohibition for anyone to censor any mail, wiretap any telecommunications, provide communication confirmation data, or record or listen to any conversation between others that are not made public, except on the basis of the CPA, the CPPA or the Military Court Act.[50] The term *"communication*" within the meaning of the CPPA covers both ordinary mail and telecommunications.[51] In this respect, the CPPA distinguishes between "*communication-restricting measures*"[52] and the collection of "*communication confirmation data*".

---

42 Article 106(3) CPA.

43 Article 219 CPA in conjunction with Article 106(4) CPA.

44 Article 216(3) CPA.

45 Article 216(3) CPA.

46 Article 216(1) and (2) CPA.

47 Article 218 CPA. As regards personal information, this only covers the voluntary production by the concerned individual him-/herself, not by a personal information controller holding such information (which would require a specific legal basis under the Personal Information Protection Act). Voluntarily produced articles are only admitted as evidence in court proceedings if there is no reasonable doubt regarding the voluntary nature of the disclosure, which it is for the prosecutor to demonstrate. See Supreme Court Decision 2013Do11233, 10 March 2016.

48 Article 308-2 CPA.

49 Article 321 Criminal Act.

50 Article 3 CPPA. The Military Court Act in principle governs the collection of information on military personnel and can only apply to civilians in a limited number of cases (e.g. if military personnel and civilians would commit a crime together, or if an individual commits a crime against the military, proceedings may be initiated before a military court, see Article 2 Military Court Act). The general provisions governing searches and seizures are similar to the CPA, see e.g. Articles 146-149 and 153-156 Military Court Act. For example, postal mail may only be collected when necessary for an investigation and on the basis of a warrant from the Military Court. To the extent that electronic communications would be collected, the limitations and safeguards of the CPPA apply.

51 Article 2(1) CPPA, i.e. "*transmission or reception of all kinds of sounds, words, symbols or images by wire, wireless, fibre cable or other electromagnetic system, including telephone, e-mail, membership information service, facsimile and radio paging*".

52 Articles 2(7) and 3(2) CPPA.

The notion of communication-restricting measures covers "*censorship*", i.e. the collection of the content of traditional postal mail, as well as "*wire-tapping*", i.e. the direct interception (acquiring or recording) of the content of telecommunications.[53] The notion of communication confirmation data covers "*data on the records of telecommunications*", which includes the date of telecommunications, their start- and end time, the number of outgoing and incoming calls as well as the subscriber number of the other party, the frequency of use, log files on the use of telecommunication services and location information (e.g. from transmission towers where signals are received).[54]

The CPPA sets out the limitations and safeguards for the collection of both types of data, and non-compliance with several of these requirements is subject to criminal penalties.[55]

2.2.2.2. Limitations and safeguards applicable to the collection of the content of communications (communication restricting measures)

The collection of the content of communications may only take place as a supplementary means of facilitating a criminal investigation (i.e. as a measure of last resort) and efforts must be made to minimise the interference with people's communication secrets.[56] In line with this general principle, communication-restricting measures may only be deployed where it is difficult to otherwise prevent the commission of a crime, arrest the criminal, or collect the evidence.[57] Law enforcement agencies collecting the content of communications must immediately cease to do so once continued access is no longer deemed to be necessary, thereby ensuring that the infringement of the privacy of communications is as limited as possible.[58]

Moreover, communication-restricting measures may only be used when there is substantial reason to suspect that certain serious crimes specifically listed in the CPPA are being planned, are being committed, or have been committed. These include crimes such as insurrection, drug-related crimes or crimes involving explosives, as well as crimes related to national security, diplomatic relations, or military bases and installations.[59] The target of a communication-restricting measure must be specific mail items or telecommunications sent or received by the suspect, or mail items or telecommunications sent or received by the suspect during a fixed period of time.[60]

Even when these requirements are met, the collection of content data may only take place on the basis of a court-issued warrant. In particular, a prosecutor may ask the court to permit the collection of content data regarding the suspect or person under investigation.[61] Similarly, a judicial police officer may apply for authorisation to a prosecutor, who in turn may request a

---

[53] "Censorship" is defined as "*opening mail without the consent of the party concerned or acquiring knowledge of, recording or withholding its contents through other means*" (Article 2(6) CPPA). "Wiretapping" means "*acquiring or recording the contents of telecommunications by listening to or communally reading the sounds, words, symbols or images of the communications through electronic and mechanical devices without the consent of the party concerned or interfering with their transmission and reception*" (Article 2(7) CPPA).

[54] Article 2(11) CPPA.

[55] Articles 16 and 17 CPPA. This applies for instance to warrantless collection, failure to keep records, failure to discontinue the collection when an emergency ceases to exist, or failure to give notice to the concerned individual.

[56] Article 3(2) CPPA.

[57] Article 5(1) CPPA.

[58] Article 2 CPPA Enforcement Decree.

[59] Article 5(1) CPPA.

[60] Article 5(2) CPPA.

[61] Article 6(1) CPPA.

warrant from the court.[62] A request for a warrant must be made in writing and must contain specific elements. In particular, it must set out (1) the substantial reasons to suspect that one of the listed crimes is planned, being committed or has been committed as well as any materials establishing a prima facie case of suspicion; (2) the communication-restricting measures as well as their target, scope, objective and effective period; and (3) the place where the measures would be executed and how they would be carried out.[63]

Where the legal requirements are satisfied, the court may grant written permission to carry out communication-restricting measures with respect to the suspect or person under investigation.[64] This warrant specifies the kinds of measures as well as their target, scope, effective period, place of execution and how they shall be carried out.[65]

Communication-restricting measures may only be carried out for a period of two months.[66] If the objective of the measures is achieved earlier within that period, the measures must be discontinued immediately. Conversely, if the required conditions are still met, a request to extend the effective period of communication-restricting measures may be filed within the two months' time limit. Such a request must include materials establishing a prima facie case for extending the measures.[67] The extended period may not exceed a total of one year, or three years for certain particularly serious crimes (e.g. crimes related to insurrection, foreign aggression, national security, etc.).[68]

Law enforcement authorities may compel the assistance of communication operators by providing them with the court's written permission.[69] Communication operators are required to cooperate and to keep the permission received in their files.[70] They may refuse cooperation when information on the targeted individual as indicated in the court's written permission (for example the individual's telephone number) is incorrect. Moreover, they are prohibited under all circumstances from disclosing passwords used for telecommunications.[71]

Anyone executing communication-restricting measures or requested to cooperate must keep records specifying the objectives of the measures, their execution, the date on which cooperation was provided and the target.[72] Records must also be kept by law enforcement authorities implementing communication-restricting measures, setting out the details and obtained outcomes.[73] Judicial police officers must provide this information by means of a report to the prosecutor when they close an investigation.[74]

When a prosecutor issues an indictment with respect to a case in which communication-restricting measures were used, or issues a disposition not to indict or arrest the relevant individual (i.e. not just a stay of prosecution), the prosecutor must notify the individual subject to the communication-restricting measures of the fact that communication-restricting measures were executed, the executing agency and the execution period. Such notice must be

62 Article 6(2) CPPA.
63 Article 6(4) CPPA and Article 4(1) CPPA Enforcement Decree.
64 Articles 6(5) and 6(8) CPPA.
65 Article 6(6) CPPA.
66 Article 6(7) CPPA.
67 Article 6(7) CPPA.
68 Article 6(8) CPPA.
69 Article 9(2) CPPA.
70 Article 15-2 CPPA and Article 12 CPPA Enforcement Decree.
71 Article 9(4) CPPA.
72 Article 9(3) CPPA.
73 Article 18(1) CPPA Enforcement Decree.
74 Article 18(2) CPPA Enforcement Decree.

provided in writing within 30 days from the disposition.[75] Notice may be deferred when it is likely to seriously endanger national security or disrupt the public safety and order, or when it is likely to result in material harm to the lives and bodies of others.[76] When intending to defer notice, the prosecutor or judicial police officer must obtain approval from the head of the District Public Prosecutor's Office.[77] Once the grounds for referral cease to exist, notice must be provided within 30 days from that moment in time.[78]

The CPPA also sets out a specific procedure for the collection of the content of communications in emergency situations. In particular, law enforcement agencies may collect the content of communications in the event that the planning or execution of organised crime or another serious crime that may directly cause death or serious injury is imminent, and an emergency exists that makes it impossible to go through the regular procedure (as set out above).[79] In such an emergency, a police officer or prosecutor may take communication-restricting measures without prior court permission but must file for court permission immediately after execution. If the law enforcement agency fails to obtain court permission within 36 hours from the moment the emergency measures were carried out, the collection must be discontinued immediately, typically followed by the destruction of the collected information.[80] Police officers carrying out emergency surveillance do so under the control of a prosecutor, or, in case receiving the prosecutor's instructions in advance is impossible due to the necessity of acting urgently, the police must obtain the approval of a prosecutor immediately upon commencing execution.[81] The rules on the notification of the individual as described above also apply to the collection of the content of communications in emergency situations.

Collection of information in emergency situations must always take place in accordance with an "*emergency censorship/wiretapping statement*" and the authority carrying out the collection must keep a register of any emergency measure.[82] The request to a court to grant permission for emergency measures must be accompanied by a written document indicating the necessary communication-restricting measures, the target, subject, scope, period, place of execution, method, and an explanation as to how the relevant communication-restricting measures meet Article 5(1) CPPA,[83] along with supporting documents.

In cases when emergency measures are completed within a short time, thus ruling out court permission (e.g. if the suspect is arrested immediately after initiating the interception, which therefore stops), the head of the competent Public Prosecutor's Office serves an emergency measure notice to the competent court.[84] The notice must set out the objective, target, scope, period, place of execution and method of collection as well as the grounds for not filing a request for court permission.[85] This notice allows the receiving court to examine the legality of the collection and must be entered into a registry of emergency measure notices.

---

75 Article 9-2(1) CPPA.
76 Article 9-2(4) CPPA.
77 Article 9-2(5) CPPA.
78 Article 9-2(6) CPPA.
79 Article 8(1) CPPA.
80 Article 8(2) CPPA.
81 Article 8(3) CPPA and Article 16(3) CPPA Enforcement Decree.
82 Article 8(4) CPPA.
83 That is, that there is a substantial reason to suspect that certain serious crimes are being planned or committed, or have been committed, and it is impracticable otherwise to prevent the commission of a crime, arrest the criminal, or collect evidence.
84 Article 8(5) CPPA.
85 Article 8(6)-(7) CPPA.

As a general requirement, the content of communications acquired through the execution of communication-restricting measures on the basis of the CPPA may only be used to investigate, prosecute or prevent the specific crimes listed above, in disciplinary proceedings for the same crimes, a claim for damages raised by a party to the communications or where this is allowed by other laws.[86]

Specific safeguards apply where telecommunications transmitted over the internet are collected.[87] Such information may only be used to investigate the serious crimes listed in Article 5(1) CPPA. To retain the information, approval must be obtained from the court that authorised the communication-restricting measures.[88] A request for retention must contain information on the communication-restricting measures, a summary of the results of the measures, the reasons for retention (together with supporting materials) and the telecommunications to be retained.[89] In the absence of such a request, the acquired telecommunications must be deleted within 14 days after the communication-restricting measures have ended.[90] If a request is rejected, the telecommunications must be destroyed within seven days.[91] Where telecommunications are deleted, a report must be filed within seven days with the court that authorised the communication-restricting measures, setting out the reasons for the deletion, as well as the details and timing thereof.

More generally, if information was illegally obtained by means of communication-restricting measures, it will not be admitted as evidence in judicial or disciplinary proceedings.[92] Also, the CPPA prohibits any person taking communication-restricting measures from disclosing confidential information obtained in the course of implementing such measures, and from using the information obtained to damage the reputation of those who are subject to the measures.[93]

2.2.2.3. Limitations and safeguards applicable to the collection of communication confirmation information

On the basis of the CPPA, law enforcement authorities may request telecommunication operators to provide communication confirmation data when necessary to conduct an investigation or execute a sentence.[94] Unlike for the collection of content data, the possibility to collect communication confirmation data is not limited to certain specific crimes. However, as is the case for content data, the collection of communication confirmation data requires prior written permission from a court, subject to the same conditions as described earlier.[95] When grounds of urgency make it impossible to obtain court permission, communication confirmation data may be collected without a warrant, in which case the permission must be obtained immediately after requesting the data and must be

86 Article 12 CPPA.
87 Article 12-2 CPPA.
88 The prosecutor or police officer executing the communication-restricting measures must select the telecommunications to be retained within 14 days after the measures end and request court approval (in the case of a police offer, the application must be made to a prosecutor, who in turn submits the request to the court), see Article 12-2(1) and (2) CPPA.
89 Article 12-2(3) CPPA.
90 Article 12-2(5) CPPA.
91 Article 12-2(5) CPPA.
92 Article 4 CPPA.
93 Article 11(2) CPPA Enforcement Decree.
94 Article 13(1) CPPA.
95 Articles 13 and 6 CPPA.

communicated to the telecommunication provider.[96] If no subsequent permission is obtained, the collected information must be destroyed.[97]

Prosecutors, judicial police officers and courts must keep records of requests for communication confirmation data.[98] In addition, telecommunication providers must twice per year report on the disclosure of communication confirmation data to the Minister of Science and ICT, and must keep records thereof for seven years from the date on which data has been disclosed.[99]

Individuals are in principle notified of the fact that communication confirmation data has been collected.[100] The timing for such notification depends on the circumstances of the investigation.[101] Once a decision is taken (not) to prosecute, notification must be provided within 30 days. Conversely, if indictment is suspended, notification must be provided within 30 days following one year after such decision is taken. In any event, notification must be provided within 30 days following one year after the information has been collected.

The notification may be deferred if it is likely to (1) endanger national security, public security and order, (2) cause death or bodily injury, (3) impede fair judicial proceedings (e.g. leading to the destruction of evidence or threatening of witnesses), or (4) defame the suspect, victims or other persons related to the case, or invade their privacy.[102] Notification on one of the aforementioned grounds requires authorisation from the director of a competent district public prosecutors' office.[103] When the grounds for deferral cease to exist, notice must be provided within 30 days from that moment in time.[104]

Notified individuals may submit a written request to the prosecutor or judicial police officer concerning the reasons for the collection of the communication confirmation data.[105] In that case, the prosecutor or judicial police officer must provide the reasons in writing within 30 days after receiving the request, unless one of the abovementioned grounds (exceptions for deferral of notification) applies.[106]

2.2.3. Voluntary disclosure by telecommunications business operators

Article 83(3) of the TBA allows telecommunications business operators to voluntarily comply with a request (made in support of a criminal trial, investigation or the execution of a sentence) from a court, prosecutor or the head of an investigative agency, to disclose "*communications data*". In the context of the TBA, "*communications data*" cover the name, resident registration number, address and phone number of users, the dates on which users subscribe or terminate their subscription as well as user identification codes (i.e. codes used to identify the rightful user of computer systems or communication networks).[107] For the purpose of the TBA, only individuals that directly contract services from a Korean

[96] Article 13(2) CPPA. As is the case for urgent communication-restricting measures, a document setting out the details of the case (the suspect, the measures to be taken, the suspected crime as well as the urgency) must be drawn up. See Article 37(5) CPPA Enforcement Decree.
[97] Article 13(3) CPPA.
[98] Article 13(5) and (6) CPPA.
[99] Article 13(7) CPPA.
[100] See Article 13-3(7), in conjunction with Article 9-2 CPPA.
[101] Article 13-3(1) CPPA.
[102] Article 13-3(2) CPPA.
[103] Article 13-3(3) CPPA.
[104] Article 13-3(4) CPPA.
[105] Article 13-3(5) CPPA.
[106] Article 13-3(6) CPPA.
[107] Article 83(3) TBA.

telecommunications provider are considered users.[108] As a consequence, situations where EU individuals whose data has been transferred to the Republic of Korea would be considered users under the TBA are likely to be very limited, as those individuals would normally not conclude a direct contract with a Korean telecommunications operator.

Requests to obtain communications data on the basis of the TBA must be made in writing and state the reasons for the request, the link to the relevant user and the scope of the requested data.[109] Where it is impossible to provide a written request due to urgency, the written request must be provided as soon as the reason for the urgency disappears.[110] Telecommunications business operators that comply with requests to disclose communications data must retain ledgers which contain records indicating that communications data have been provided, as well as the related materials, such as the written request.[111] Moreover, telecommunications business operators must report on the provision of communications data to the Minister of Science and ICT twice per year.[112]

There is no obligation for telecommunications business operators to comply with requests to disclose communications data on the basis of the TBA. Each request must therefore be assessed by the operator in light of the applicable data protection requirements under PIPA. In particular, a telecommunications business operator must take into account the interests of the data subject and may not disclose the information if it would be likely to infringe unfairly on the interest of the individual or a third party.[113] In addition, in accordance with Notification No. 2021-1 on Supplementary rules for the interpretation and application of the Personal Information Protection Act, the concerned individual must be notified of the disclosure. In exceptional situations, such notification may be delayed, in particular if and for as long as the notification would jeopardise an ongoing criminal investigation or is likely to harm the life or body of another person, where those rights or interests are manifestly superior to the rights of the data subject.[114]

In 2016, the Supreme Court confirmed that the voluntary provision of communications data by telecommunications business operators without a warrant on the basis of the TBA does not as such violate the right to informational self-determination of the user of the telecommunication service. At the same time, the Court clarified that there would be such a violation if it is manifestly apparent that the requesting agency abused its authority to request the disclosure of communications data, thereby violating the interests of the individual concerned or a third party.[115] More generally, any request for voluntary disclosure by a law enforcement authority must comply with the principles of lawfulness, necessity and proportionality following from the Korean Constitution (Articles 12(1) and 37(2)).

2.3. Oversight

Oversight of criminal law enforcement authorities is carried out through different mechanisms, both internally and by external bodies.

2.3.1. Self-auditing

[108] Article 2(9) TBA.
[109] Article 83(4) TBA.
[110] Article 83(4) TBA.
[111] Article 83(5) TBA.
[112] Article 83(6) TBA.
[113] Article 18(2) PIPA.
[114] Notification No. 2021-1 of the PIPC on Supplementary rules for the interpretation and application of the Personal Information Protection Act, Section III, 2, (iii).
[115] Supreme Court Decision No. 2012Da105482, 10 March 2016.

In accordance with the Act on Public Sector Audits, public authorities are encouraged to establish an internal body for self-auditing, with the task, amongst others, to carry out legality control.[116] The heads of such audit bodies must be guaranteed independence to the largest extent possible.[117] More specifically, they are appointed from outside the relevant authority (e.g. former judges, professors) for a period of two to five years and can only be dismissed for justified reasons (e.g. when unable to perform duties due to a mental or physical disorder, when subject to disciplinary action).[118] Likewise, auditors are appointed on the basis of specific conditions laid down in the Act.[119] Audit reports may include recommendations or requests for compensation or correction, as well as reprimands and recommendations or requests for disciplinary action.[120] They are notified to the head of the public authority subject to the audit, as well as to the Board of Audit and Inspection (see section 2.3.2) within 60 days from completion of the audit.[121] The authority concerned must implement the required measures and report the results to the Board of Audit and Inspection.[122] In addition, audit results are generally made available to the public.[123] The refusal or obstruction of a self-audit is subject to administrative fines.[124] In the area of criminal law enforcement, to comply with the aforementioned legislation, the National Police Agency operates an Inspector-General system to handle internal audits, including with respect to possible human rights violations.[125]

2.3.2. The Board of Audit and Inspection

The Board of Audit and Inspection (hereafter "*BAI*") may inspect the activities of public authorities and, on the basis of such inspections, issue recommendations, request disciplinary actions, or file a criminal complaint.[126] The BAI is established under the President of the Republic of Korea, but retains an independent status with respect to its duties.[127] In addition, the Act establishing the BAI requires that the BAI shall be granted independence to the maximum extent with respect to the appointment, dismissal and organisation of its staff, as well as the compilation of its budget.[128] The Chairperson of the BAI is appointed by the President, with the consent of the National Assembly.[129] The six remaining Commissioners are appointed by the President, upon recommendation of the Chairperson, for a four-year term.[130] Commissioners (including the Chairperson) must meet specific qualifications laid down by law[131] and may only be dismissed in case of impeachment, sentencing to imprisonment or inability to perform their duties due to long-term mental or physical

---

116 Articles 3 and 5 Act on Public Sector Audits.
117 Article 7 Act on Public Sector Audits.
118 Articles 8-11 Act on Public Sector Audits.
119 Articles 16 et seq. Act on Public Sector Audits.
120 Article 23(2) Act on Public Sector Audits.
121 Article 23(1) Act on Public Sector Audits.
122 Article 23(3) Act on Public Sector Audits.
123 Article 26 Act on Public Sector Audits.
124 Article 41 Act on Public Sector Audits.
125 See in particular the divisions under the Director General for Audit and Inspection: https://www.police.go.kr/eng/knpa/org/org01.jsp.
126 Articles 24 and 31-35 Board of Audit and Inspection Act (hereafter "*BAI Act*").
127 Article 2(1) BAI Act.
128 Article 2(2) BAI Act.
129 Article 4(1) BAI Act.
130 Articles 5(1) and 6 BAI Act.
131 E.g. having served as a judge, public prosecutor or attorney-at-law for at least ten years, worked as a public servant, or professor or higher-ranking position at a university for at least eight years, or worked for at least ten years in a stock-listed corporation or government-invested institution (of which at least five years as an executive officer), see article 7 BAI Act.

weakness.[132] Moreover, Commissioners are prohibited from participating in political activities, and from concurrently holding offices in the National Assembly, administrative agencies, organisations subject to audit and inspection by the BAI or any other office or position that is remunerated.[133]

The BAI conducts a general audit on an annual basis, but may also conduct specific audits on matters of special interest. The BAI may request the submission of documents in the course of an inspection and request the attendance of individuals.[134] As part of an audit, the BAI examines the revenue and expenditure of the State, but also oversees general compliance with the duties of public authorities and public officials with a view to improving the operation of public administration.[135] Its oversight therefore extends beyond budgetary aspects and also includes a legality control.

2.3.3. The National Assembly

The National Assembly may investigate and inspect public authorities.[136] During an investigation or inspection, the National Assembly may request the disclosure of documents and compel the appearance of witnesses.[137] Anyone committing perjury during an investigation of the National Assembly is subject to criminal sanctions (imprisonment for up to ten years).[138] The process and results of inspections may be made public.[139] If the National Assembly finds unlawful or improper activity, it may request that the relevant public authority takes corrective measures, including awarding compensation, taking disciplinary action, and improving its internal procedures.[140] Following such a request, the authority must act without delay and report the outcome to the National Assembly.[141]

2.3.4. The Personal Information Protection Commission

The Personal Information Protection Commission (hereafter "*PIPC*") exercises oversight over the processing of personal information by criminal law enforcement authorities in line with PIPA. In addition, according to Article 7-8(3), (4) and Article 7-9(5) PIPA, the oversight of the PIPC also covers possible infringements of the rules setting out the limitations and safeguards with respect to the collection of personal information, including those contained in the specific laws regulating the collection of (electronic) evidence for the purposes of criminal law enforcement (see section 2.2). Given the requirements in Article 3(1) PIPA for the lawful and fair collection of personal information, any such infringement also constitutes a violation of PIPA, allowing the PIPC to carry out an investigation and to take corrective measures.[142]

---

[132] Article 8 BAI Act.
[133] Article 9 BAI Act.
[134] See e.g. Article 27 BAI Act.
[135] Articles 20 and 24 BAI Act.
[136] Article 128 National Assembly Act and Articles 2, 3 and 15 Act on the Inspection and Investigation of State Administration. This includes annual inspections of government affairs as a whole and investigations of specific matters.
[137] Article 10(1) Act on the Inspection and Investigation of State Administration. See also Articles 128 and 129 National Assembly Act.
[138] Article 14 Act on Testimony, Appraisal, etc. before the National Assembly.
[139] Article 12-2 Act on the Inspection and Investigation of State Administration.
[140] Article 16(2) Act on the Inspection and Investigation of State Administration.
[141] Article 16(3) Act on the Inspection and Investigation of State Administration.
[142] See PIPC Notification No. 2021-1 on Supplementary rules for the interpretation and application of the Personal Information Protection Act.

In exercising its oversight function, the PIPC has access to all relevant information.[143] The PIPC may provide advice to law enforcement authorities to improve the level of personal information protection of their processing activities, impose corrective measures (e.g. to suspend data processing or take necessary measures to protect personal information) or advise the authority to take disciplinary action.[144] Finally, criminal sanctions are foreseen for certain PIPA violations, such as unlawfully using or disclosing personal information to third parties or the unlawful processing of sensitive information.[145] In this respect, the PIPC may refer the matter to the competent investigative agency (including a prosecutor).[146]

2.3.5. The National Human Rights Commission

The National Human Rights Commission (hereafter "*NHRC*") – an independent body tasked with protecting and promoting fundamental rights[147] – has the power to investigate and remedy violations of Articles 10–22 of the Constitution, which include the rights to privacy and privacy of correspondence. The NHRC is comprised of 11 Commissioners, appointed upon nomination by the National Assembly (four), the President (four) and the Chief Justice of the Supreme Court (three).[148] To be appointed, a Commissioner must (1) have served for at least ten years at a university or an authorized research institute, at least as an associate professor; (2) have served as a judge, prosecutor, or attorney-at-law for at least ten years; (3) have been engaged in human rights activities for at least ten years (e.g. for a non-profit, non-governmental organisation or international organisation); or (4) have been recommended by civil society groups.[149] The Chairperson is appointed by the President from among the Commissioners and must be confirmed by the National Assembly.[150] Commissioners (including the Chairperson) are appointed for a renewable term of three years and may only be dismissed in case they are sentenced to imprisonment or are no longer capable of performing their duties due to prolonged physical or mental weakness (in which case two thirds of the Commissioners must agree to the dismissal).[151] NHRC Commissioners are prohibited from holding a concurrent office in the National Assembly, local councils, or any State or local government (as a public official).[152]

The NHRC may initiate an investigation on its own initiative or on the basis of a petition from an individual. As part of its investigation, the NHRC may request the submission of relevant materials, conduct inspections and summon individuals to testify.[153] Following an investigation, the NHRC may issue recommendations to improve or correct specific policies and practices, and may make them public.[154] Public authorities must notify the NHRC of a plan to implement such recommendations within 90 days upon receiving them.[155] Moreover,

---

143 Article 63 PIPA.
144 Articles 61(2), 65(1), 65(2) and 64(4) PIPA.
145 Articles 70-74 PIPA.
146 Article 65(1) PIPA.
147 Article 1 Human Rights Commission Act (hereafter "*NHRC Act*").
148 Article 5(1) and (2) NHRC Act.
149 Article 5(3) NHRC Act.
150 Article 5(5) NHRC Act.
151 Article 7(1) and Article 8 NHRC Act.
152 Article 10 NHRC Act.
153 Article 36 NHRC Act. In accordance with Article 36(7) of the Act, the submission of materials or articles may be rejected if it would prejudice state confidentiality liable to have a substantial effect on state security or diplomatic relations or would present a serious obstacle to a criminal investigation or pending trial. In such cases, the Commission may request further information from the head of the relevant agency (which has to comply in good faith) where necessary to review whether the refusal to provide the information is justified.
154 Article 25(1) NHRC Act.
155 Article 25(3) NHRC Act.

in case of a failure to implement recommendations, the concerned authority must inform the Commission thereof.[156] The NHRC may in turn disclose such failure to the National Assembly, and/or make it public. Public authorities generally comply with NHRC recommendations and have a strong incentive to do so as their implementation has been assessed as part of the general evaluation conducted by the Office for Government Policy Coordination, under the authority of the Prime Minister's Office.

2.4. Individual redress

2.4.1. Redress mechanisms available under PIPA

Individuals may exercise their rights of access, correction, deletion and suspension under PIPA with respect to personal information processed by criminal law enforcement authorities. Access may be requested directly from the relevant authority, or indirectly via the PIPC.[157] The competent authority may limit or deny access only where this is provided for by law, where it would likely cause damage to the life or body of a third party, or would likely lead to or unjustified infringement of property and other interests of another person (i.e. where the interests of the other person would outweigh the interests of the individual making the request).[158] If an access request is denied, the individual must be informed of the reasons therefor and how to appeal.[159] Similarly, a request for correction or erasure may be denied where this is provided for in other laws, in which case the individual must be informed of the underlying reasons and the possibility to appeal.[160]

As regards redress, individuals may lodge a complaint with the PIPC, including through the Privacy Call Centre operated by the Korea Internet and Security Agency.[161] In addition, an individual may obtain mediation through the Personal Information Dispute Mediation Committee.[162] These redress avenues are available both in case of possible infringements of the rules contained in specific laws setting out the limitations and safeguards with respect to the collection of personal information (section 2.2) and of PIPA. In addition, individuals may challenge the decisions or inaction of the PIPC under the Administrative Litigation Act (see section 2.4.3).

2.4.2. Redress before the National Human Rights Commission

The NHRC handles complaints from individuals (both Korean and foreign nationals) concerning human rights violations committed by public authorities.[163] There is no standing requirement for individuals to lodge a complaint with the NHRC.[164] As a consequence, a

---

156 Article 25(4) NHRC Act.
157 Article 35(2) PIPA.
158 Article 35(4) PIPA.
159 Article 42(2) PIPA Enforcement Decree.
160 Article 36(1)-(2) PIPA and Article 43(3) PIPA Enforcement Decree.
161 Article 62 PIPA.
162 Articles 40-50 PIPA and Articles 48-2 to 57 PIPA Enforcement Decree.
163 Although Article 4 NHRC Act refers to citizens and foreigners residing in the Republic of Korea, the term "residing" reflects a concept of jurisdiction rather than territory. Therefore, if the fundamental rights of a foreigner outside of Korea are violated by national institutions within Korea, that individual may file a complaint with the NHRC. See for example the corresponding question on the NHRC's Frequently Asked Questions page, available at https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2. This would be the case if personal data of a foreigner transferred to Korea is unlawfully accessed by Korean public authorities.
164 A complaint must in principle be filed within one year from the violation, but the NHRC may still decide to investigate a complaint that is lodged after that time period as long as the statute of limitation under criminal or civil law has not expired (Article 32(1) lit. 4 NHRC Act).

complaint will be handled by the NHRC even if the concerned individual cannot demonstrate an injury in fact at the admissibility stage. In the context of the collection of personal data for criminal law enforcement purposes, an individual would therefore not be required to demonstrate that his/her personal information has in fact been accessed by Korean public authorities for the complaint to be admissible before the NHRC. An individual may also request to resolve the complaint through mediation.[165]

To investigate a complaint, the NHRC can make use of its investigatory powers, including by requesting the submission of relevant materials, conducting inspections and summoning individuals to testify.[166] If the investigation reveals that a violation of relevant laws has occurred, the NHRC may recommend the implementation of remedies or the rectification or improvement of any relevant statute, institution, policy or practice.[167] Proposed remedies may include mediation, cessation of the human rights violation, compensation for damages and measures to prevent recurrence of the same or similar violations.[168] In the case of unlawful collection of personal information under applicable rules, remedial measures may include the deletion of the personal information collected. If it is deemed highly likely that the infringement is ongoing and it is deemed likely that, if left unattended, damage difficult to remedy would be caused, the NHRC may adopt urgent relief measures.[169]

While the NHRC has no power to compel, its decisions (e.g. a decision not to continue the investigation of a complaint)[170] and recommendations can be challenged before the Korean courts under the Administrative Litigation Act (see section 2.4.3 below).[171] In addition, if the findings of the NHRC reveal that personal data was unlawfully collected by a public authority, an individual could seek further redress before the Korean courts against that public authority, e.g. by challenging the collection under the Administrative Litigation Act, filing a constitutional complaint under the Constitutional Court Act, or applying for compensation of damages under the State Compensation Act (see section 2.4.3 below).

2.4.3. Judicial redress

Individuals may invoke the limitations and safeguards described in the previous sections to obtain redress before the Korean courts through different avenues.

First, in accordance with the CPA, the concerned individual and his/her counsel may be present when a warrant for a search or seizure is being executed, and may therefore raise an objection at the time the warrant is being executed.[172] In addition, the CPA provides for a so-called "quasi-complaint" mechanism, which allows individuals to petition the competent court with a request to cancel or alter a disposition made by a prosecutor or police officer

[165] Articles 42 et seq. NRHC Act.
[166] Articles 36 and 37 NHRC Act.
[167] Article 44 NHRC Act.
[168] Article 42(4) NHRC Act.
[169] Article 48 NHRC Act.
[170] For example, if the NHRC is exceptionally not able to inspect certain materials or facilities because they concern state secrets liable to have a substantial effect on state security or diplomatic relations, or where the inspection would present a serious obstacle to a criminal investigation or pending trial (see footnote 166), and where this prevents the NHRC from carrying out the investigation necessary to assess the merits of the petition received, it will inform the individual of the reasons why the complaint was rejected, in accordance with Article 39 NHRC Act. In this case, the individual could challenge the NHRC's decision under the Administrative Litigation Act.
[171] See e.g. Seoul High Court Decision 2007Nu27259, 18 April 2008, confirmed by Supreme Court Decision 2008Du7854, 9 October 2008; Seoul High Court Decision 2017Nu69382, 2 February 2018.
[172] Articles 121 and 219 CPA

concerning a seizure.[173] This allows individuals to challenge the measures taken to execute a seizure warrant.

Moreover, individuals may obtain compensation for damages before the Korean courts. On the basis of the State Compensation Act, individuals may apply for compensation for damages inflicted by public officials in performing their official duties in violation of the law.[174] A claim under the State Compensation Act may be filed with a specialised "Compensation Council", or directly with the Korean courts.[175] If the victim is a foreign national, the State Compensation Act applies as long as that national's country of origin equally ensures state compensation for Korean nationals.[176] According to case law, this condition is fulfilled if the requirements to request compensation in the other country "*are not significantly off-balanced between Korea and the other country*" and "*are not generally stricter than those determined by Korea, having no material and substantive difference.*"[177] The Civil Act governs the state's liability for compensation and, as a consequence, state liability also covers non-property damages (e.g. mental suffering).[178]

For violations of the data protection rules, an additional legal remedy is provided under PIPA. According to Article 39 PIPA, any individual suffering harm as a result of a violation of PIPA or of a loss, theft, divulgence, forgery, alteration of, or damage to his/her personal information may obtain compensation for damages before the courts. There is no similar requirement of reciprocity as under the State Compensation Act.

In addition to compensation for damages, administrative redress may be obtained against actions or omissions of administrative agencies under the Administrative Litigation Act. Any individual may challenge a disposition (i.e. the exercise of, or refusal to exercise, public power in a specific case) or omission (the prolonged failure of an administrative agency to take a certain disposition contrary to a legal obligation to do so), which may lead to the revocation/alteration of an illegal disposition, a finding of nullity (i.e. a finding that the disposition does not have legal effect or its non-existence in the legal order) or a finding that an omission is illegal.[179] In order to be able to challenge an administrative disposition, it must directly impact on civil rights and duties.[180] This includes measures to collect personal data, be it directly (e.g. intercepting communications) or by way of a disclosure request (e.g. to a service provider).

The aforementioned claims may first be brought before administrative appeals commissions established under certain public authorities (e.g. the NIS, the NHRC) or before the Central

[173] Article 417 CPA in conjunction with Article 414(2) CPA. See also Supreme Court Decision No. 97Mo66, 29 September 1997.

[174] Article 2(1) State Compensation Act.

[175] Articles 9 and 12 State Compensation Act. The Act establishes District Councils (chaired by the deputy prosecutor of the corresponding prosecutor's office), a Central Council (chaired by the Vice Minister of Justice) and a Special Council (chaired by the Vice Minister of National Defense and in charge of compensation claims for damages inflicted by military personnel or civilian employees of the military). Claims for compensation are in principle handled by District Councils, which under certain circumstances have to forward cases to the Central/Special Council, e.g. if the compensation exceeds a certain amount or in case an individual applies for re-deliberation. All Councils consist of members appointed by the Minister of Justice (e.g. from among public officials of the Ministry of Justice, judicial officers, lawyers, and persons having an expertise in in relation to state compensation) and are subject to specific rules on conflict of interest (see Article 7 Enforcement Decree of the State Compensation Act).

[176] Article 7 State Compensation Act.

[177] Supreme Court Decision No. 2013Da208388, 11 June 2015.

[178] See Article 8 State Compensation Act, as well as Article 751 Civil Act.

[179] Articles 2 and 4 Administrative Litigation Act.

[180] Supreme Court Decision 98Du18435, 22 October 1999, Supreme Court Decision 99Du1113, 8 September 2000, and Supreme Court Decision 2010Du3541, 27 September 2012.

Administrative Appeals Commission established under the Anti-Corruption and Civil Rights Commission.[181] Such an administrative appeal provides an alternative, more informal avenue to challenge a disposition or omission of a public authority. However, a claim may also be brought directly before the Korean courts, under the Administrative Litigation Act.

A request for revocation/alteration of a disposition under the Administrative Litigation Act may be filed by any person having a legal interest to seek the revocation/alteration, or to be restored in his/her rights by the revocation/alteration in case the disposition no longer has effect.[182] Similarly, litigation to affirm nullity may be brought by a person having a legal interest in such affirmation, while a litigation to affirm the illegality of an omission may be initiated by any person who has made a request for a disposition and has a legal interest to seek that the illegality of the omission be affirmed.[183] According to case law of the Supreme Court, "legal interest" is interpreted as a "legally protected interest", i.e. a direct and specific interest protected by laws and regulations on which administrative dispositions are based (i.e. not general, indirect and abstract interests of the public).[184] Individuals therefore have a legal interest in case of any violation of the limitations and safeguards with respect to the collection of their personal data for criminal law enforcement purposes (under specific laws or PIPA). A final judgment under the Administrative Litigation Act is binding on the parties.[185]

A request for revocation/alteration of a disposition and a request to affirm the illegality of an omission must be filed within 90 days from the date the individual becomes aware of the disposition/omission and in principle no later than one year from the date the disposition is issued/omission occurred, unless there are justifiable reasons.[186] According to the case law of the Supreme Court, the notion of "justifiable reasons" is to be interpreted broadly and requires assessing whether it is socially acceptable to allow a delayed complaint, in light of all the circumstances of the case.[187] For example, this includes (but is not limited to) reasons for delay for which the concerned party cannot be held responsible (i.e. situations that are outside the control of the complainant, for instance where (s)he has not been notified of the collection of his/her personal information) or force majeure (e.g. natural disaster, war).

Finally, individuals may also file a constitutional complaint with the Constitutional Court.[188] On the basis of the Constitutional Court Act, any person whose fundamental rights guaranteed by the Constitution are infringed due to the exercise or non-exercise of governmental power (excluding judgments of the courts), may request adjudication of a constitutional complaint. If other remedies are available, these must be exhausted first. According to the case law of the Constitutional Court, foreign nationals may file a constitutional complaint to the extent their basic rights are recognised under the Korean Constitution (see the explanations in section 1.1).[189] Constitutional complaints must be filed within 90 days after the individual has become aware of the infringement, and within one year after its occurrence. Given that the procedure of the Administrative Litigation Act is applied to litigation under the Constitutional Court Act,[190] a complaint will still be admissible

[181] Article 6 Administrative Appeals Act and Article 18(1) Administrative Litigation Act.
[182] Article 12 Administrative Litigation Act.
[183] Articles 35 and 36 Administrative Litigation Act.
[184] Supreme Court Decision No. 2006Du330, 26 March 2006.
[185] Article 30(1) Administrative Litigation Act.
[186] Article 20 Administrative Litigation Act. This time limit also applies to a claim to affirm the illegality of an omission, see Article 38(2) Administrative Litigation Act.
[187] Supreme Court Decision 90Nu6521, 28 June 1991.
[188] Article 68(1) Constitutional Court Act.
[189] Constitutional Court Decision No. 99HeonMa194, 29 November 2001.
[190] Article 40 Constitutional Court Act.

if there are "justifiable reasons", as interpreted in accordance with the Supreme Court case law described above.

If other remedies need to be exhausted first, a constitutional complaint must be filed within 30 days after the final decision on such a remedy.[191] The Constitutional Court may invalidate the exercise of governmental power that caused the infringement or confirm that a certain failure to act is unconstitutional.[192] In that case, the relevant authority is required to take measures to comply with the decision of the Court.

3. GOVERNMENT ACCESS FOR NATIONAL SECURITY PURPOSES

3.1. Competent public authorities in the area of national security

The Republic of Korea has two dedicated intelligence agencies: the NIS and the Defense Security Support Command. Beyond that, the police and prosecution may also collect personal information for national security purposes.

The NIS is established by the National Intelligence Service Act (hereafter "*NIS Act*") and operates directly under the jurisdiction and supervision of the President.[193] In particular, the NIS collects, compiles and distributes information on foreign countries (and North Korea)[194], intelligence related to the task of countering espionage (including military and industrial espionage), terrorism and the activities of international crime syndicates, intelligence on certain types of crime directed against public and national security (e.g. domestic insurrection, foreign aggression) and intelligence related to the task of ensuring cyber security and preventing or countering cyberattacks and threats.[195] The NIS Act, which establishes the NIS and sets out its tasks, also provides general principles that frame all of its activities. As a general principle, the NIS must maintain political neutrality and protect the freedom and rights of individuals.[196] The President of the NIS is charged with developing general guidelines that set out the principles, scope and procedures for the performance of the NIS' duties in relation to the collection and use of information, and has to report them to the National Assembly.[197] The National Assembly (through its Intelligence Committee) may require the guidelines to be corrected or supplemented if it considers that they are illegal or unjust. More generally, when carrying out their duties, the Director and NIS personnel may not force any institution, organisation or individual to do anything they are not obligated to do, nor obstruct any person's exercise of rights, by abusing their official authority.[198] In addition, any censorship of mail, interception of telecommunications, collection of location information, collection of communication confirmation data or the recording of or listening in on private communications by the NIS must comply with the CPPA, Location Information Act or CPA.[199] Any abuse of power or the collection of information in violation of these laws is subject to criminal sanctions.[200]

The Defense Security Support Command is a military intelligence agency, established under the Ministry of Defense. It is responsible for security matters within the military, military

[191] Article 69 Constitutional Court Act.
[192] Article 75(3) Constitutional Court Act.
[193] Articles 2 and 4(2) NIS Act.
[194] This notion does not cover information on individuals, but information on general information on foreign countries (trends, developments) and on the activities of third country state actors.
[195] Article 3(1) NIS Act.
[196] Articles 3(1), 6(2), 11, 21. See also the rules on conflicts of interest, in particular Articles 10, 12.
[197] Article 4(2) NIS Act.
[198] Article 13 NIS Act.
[199] Article 14 NIS Act.
[200] Articles 22 and 23 NIS Act.

criminal investigations (subject to the Military Court Act) and military intelligence. In general, the Defense Security Support Command does not carry out surveillance of civilians, unless this is necessary to conduct its military functions. Persons that may be investigated are military personnel, civilian employees of the military, persons in military training, persons in military reserve or recruit service and prisoners of war.[201] When collecting communication information for national security purposes, the Defense Security Support Command is subject to the limitations and safeguards laid down by the CPPA and its Enforcement Decree.

3.2. Legal bases and limitations

The CPPA, the Act on Anti-Terrorism for the Protection of Citizens and Public Security (hereafter "*Anti-Terrorism Act*") and the TBA provide legal bases for the collection of personal information for national security purposes and set out the applicable limitations and safeguards.[202] These limitations and safeguards, as described in the next sections, ensure that the collection and processing of information is limited to what is strictly necessary to achieve a legitimate objective. This excludes any mass and indiscriminate collection of personal information for national security purposes.

3.2.1. Collection of communication information

3.2.1.1. Collection of communication information by intelligence agencies

3.2.1.1.1. Legal basis

The CPPA empowers intelligence agencies to collect communication data and requires communication providers to cooperate with requests from those agencies.[203] As described in section 2.2.2.1, the CPPA distinguishes between the collection of the content of communications (i.e. "*communication-restricting measures*" such as "*wire-tapping*" or "*censorship*"[204] measures), and the collection of "*communication confirmation data*".[205]

The threshold for collecting these two types of information differs, but the applicable procedures and safeguards are to a large extent identical.[206] The collection of communication confirmation data (or meta-data) may take place for the purpose of preventing threats to national security.[207] A higher threshold applies for the execution of communication-restricting measures (i.e. to collect the content of communications), which may only be taken when national security is expected to be put in grave danger and the collection of intelligence is necessary to prevent such danger (i.e. if there is a grave risk to national security and the collection is necessary to prevent it).[208] Moreover, access to the content of communications may only be carried out as a measure of last resort to ensure national security, and efforts must be made to minimize the violation of the privacy of communications.[209] Even when the appropriate approval/permission has been obtained, such measures must be stopped

[201] Article 1 Military Court Act.
[202] When investigating crimes related to national security, the Police and NIS will act on the basis of the CPA, while the Defense Security Support Command is subject to the Military Court Act.
[203] Article 15-2 CPPA.
[204] Article 2(6) and (7) CPPA.
[205] Article 2(11) CPPA.
[206] See also Article 13-4(2) CPPA and Article 37(4) CPPA Enforcement Decree, which stipulate that the procedures applicable to the collection of the content of communications apply mutatis mutandis to the collection of communication confirmation data.
[207] Article 13-4 CPPA.
[208] Article 7(1) CPPA.
[209] Article 3(2) CPPA.

immediately once they are no longer necessary, thereby ensuring that any infringement of the individual's communication secrets is limited to the minimum.[210]

3.2.1.1.2. Limitations and safeguards applying to the collection of communication information involving at least one Korean national

The collection of communication information (both content and meta-data) where either one or both individuals involved in the communication are Korean nationals may only take place with the permission from a senior Chief Justice of the High Court.[211] The request from the intelligence agency must be made in writing to a prosecutor or a High Prosecutors' Office.[212] It must indicate the reasons for the collection (i.e. that the national security is expected to be put in grave danger, or that the collection is necessary for preventing threats to national security), together with the materials supporting those reasons and establishing a prima facie case, as well as the details of the request (i.e. the objectives, targeted individual(s), scope, effective period of collection, as well as how and where the collection will take place).[213] The prosecutor/High Prosecutors' Office in turn requests permission from a senior Chief Justice of the High Court.[214] The Chief Justice may only grant written permission when (s)he deems the application justified and will dismiss the request when (s)he considers it groundless.[215] The warrant specifies the type, objective, target, scope and effective period of collection, as well as where and how it may take place.[216]

Specific rules apply in the event that the measure aims at the investigation of an act of conspiracy that threatens national security and an emergency exists that makes it impossible to go through the aforementioned procedures.[217] When these conditions are fulfilled, intelligence agencies may carry out surveillance measures without prior court approval.[218] However, immediately after the execution of the emergency measures, the intelligence agency must request the permission of the court. If permission is not obtained within 36 hours from the time the measures are taken, they must be discontinued immediately.[219] The collection of information in emergency situations must always take place in accordance with an "emergency censorship/wiretapping statement" and the intelligence agency carrying out the collection must keep a register of any emergency measure.[220]

In cases where the surveillance is completed within a short time, ruling out court permission, the head of the competent High Prosecutors' Office must send an emergency measure notice prepared by the intelligence agency to the head of the competent court, which retains the emergency measure registry.[221] This allows the court to examine the legality of the collection.

---

[210] Article 2 CPPA Enforcement Decree.

[211] Article 7(1)1 CPPA. The competent court is the high court having jurisdiction over the place of domicile or seat of one or both parties subject to the surveillance.

[212] Article 7(3) CPPA Enforcement Decree.

[213] Articles 7(3) and 6(4) CPPA.

[214] Articles 7(4) CPPA Enforcement Decree. The prosecutor's request to the court must set out the main grounds for suspicion and, to the extent that several permissions are requested at the same time, the justification therefor (see Article 4 CPPA Enforcement Decree).

[215] Articles 7(3), 6(5) and 6(9) CPPA.

[216] Articles 7(3) and 6(6) CPPA.

[217] Article 8 CPPA.

[218] Article 8(1) CPPA.

[219] Article 8(2) CPPA.

[220] Article 8(4) CPPA. See above section 2.2.2.2. for emergency measures in the context of law enforcement.

[221] Article 8(5) and (7) CPPA. This notice must indicate the objective, target, scope, period, place of execution and method of surveillance, as well as the grounds for not filing a request before taking the measure (Article 8(6) CPPA).

3.2.1.1.3. Limitations and safeguards applying to the collection of communication information involving only non-Korean nationals

To collect information on communications exclusively between non-Korean nationals, intelligence agencies must obtain prior written approval from the President.[222] Such communications will only be collected for national security purposes if they fall within one of several listed categories, i.e. communications between government officials or other individuals of countries hostile to the Republic of Korea, foreign agencies, groups or nationals suspected of engaging in anti-Korean activities,[223] or members of groups within the Korean Peninsula effectively beyond the sovereignty of the Republic of Korea and their umbrella groups based in foreign countries.[224] Conversely, if one party to a communication is a Korean national and the other a non-Korean national, court approval will be required in accordance with the procedure described in section 3.2.1.1.2.

The head of an intelligence agency must submit a plan for the measures intended to be taken to the Director of the NIS.[225] The Director of the NIS reviews whether the plan is appropriate and, if this is the case, submits it for approval to the President.[226] The information that must be included in the plan is the same as the information required for an application for court permission to collect information of Korean nationals (as described above).[227] In particular, it must indicate the reasons for the collection (i.e. that the national security is expected to be put in grave danger, or that the collection is necessary for preventing threats to national security), the main grounds for suspicion, together with the materials supporting those reasons and establishing a prima facie case, as well as the details of the request (i.e. the objectives, targeted individual(s), scope, effective period of collection, as well as how and where the collection will take place). Where several permits are requested at the same time, the purport and grounds thereof.[228]

In emergency situations,[229] prior approval from the Minister to whom the relevant intelligence agency belongs must be obtained. However, in this case the intelligence agency must request the approval of the President immediately after the emergency measures have been taken. If an intelligence agency fails to obtain approval within 36 hours from the time the application is made, the collection must be discontinued immediately.[230] In such cases, the collected information will always be destroyed.

3.2.1.1.4. General limitations and safeguards

When requesting the cooperation of private entities, intelligence agencies have to provide them with the court warrant/presidential permission or a copy of the cover of an emergency censorship statement, which the compelled entity must keep in its files.[231] Entities requested

---

[222] Article 7(1)2 CPPA.

[223] This refers to activities that threaten the nation's existence and safety, democratic order or the people's survival and freedom.

[224] Moreover, if one party is a person described in Article 7(1)2 CPPA and the other is unknown or cannot be specified, the procedure prescribed by Article 7(1)2 will apply.

[225] Article 8(1) CPPA Enforcement Decree. The Director of the NIS is appointed by the President following confirmation by the Parliament (Article 7 NIS Act).

[226] Article 8(2) CPPA Enforcement Decree.

[227] Article 8(3) CPPA Enforcement Decree, in conjunction with Article 6(4) CPPA.

[228] Articles 8(3) and 4 CPPA Enforcement Decree.

[229] That is, in cases when the measure aims at an act of conspiracy that threatens national security, there is insufficient time to obtain approval of the President and failure to adopt emergency measures may harm national security (Article 8(8) CPPA).

[230] Article 8(9) CPPA.

[231] Article 9(2) CPPA and Article 12 CPPA Enforcement Decree.

to disclose information to intelligence agencies on the basis of the CPPA may refuse to do so when the authorisation or emergency censorship statement refers to the wrong identifier (e.g. a telephone number belonging to a different individual than the one identified). Moreover, in all cases, passwords used for communications may not be disclosed.[232]

Intelligence agencies may entrust the implementation of communication-restricting measures or the collection of communication confirmation information to a post office or a telecommunications service provider (as defined by the Telecommunications Business Act).[233] Both the relevant intelligence agency and the provider receiving a request to cooperate must keep registries indicating the purpose of requesting the measures, the date of execution or cooperation, and the object of the measures (e.g. mail, telephone, email) for three years.[234] Telecommunications service providers providing communication confirmation data have to keep information on the frequency of collection in their files for seven years and report twice per year to the Minister of Science and ICT.[235]

Intelligence agencies have to report on the information they have gathered and the outcome of the surveillance activity to the Director of the NIS.[236] With respect to the collection of communication confirmation data, records must be kept of the fact that a request for such data was made, as well as the written request itself and the institution that relied on it.[237]

The collection of both the content of communications and communication confirmation data may only last for a maximum period of four months and, if the pursued objective is achieved in the meantime, must be discontinued immediately.[238] If the conditions for permission persist, the period may be extended for up to four months, with the court's permission or President's approval. The application to obtain approval to extend the surveillance measures must be made in writing, stating the reasons why extension is sought and providing supporting materials.[239]

Depending on the legal basis for collection, individuals are generally notified when their communications are collected. In particular, regardless of whether the information collected concerns the content of communications or communication confirmation data and regardless of whether the information was obtained through the ordinary procedure or in an emergency situation, the head of the intelligence agency must notify the individual concerned of the surveillance measure in writing within 30 days from the date on which the surveillance ended.[240] The notification must include (1) the fact that the information has been collected, (2) the executing agency and (3) the execution period. However, if it is likely that the notice would put national security at risk or would harm people's life and physical safety, the notice may be deferred.[241] Notice must be given within 30 days once the grounds for deferral cease to exist.[242]

---

[232] Article 9(4) CPPA.
[233] Article 13 CPPA Enforcement Decree.
[234] Article 9(3) CPPA and Article 17(2) CPPA Enforcement Decree. This time period does not apply to communication confirmation data (see Article 39 CPPA Enforcement Decree).
[235] Article 13(7) CPPA and Article 39 CPPA Enforcement Decree.
[236] Article 18(3) CPPA Enforcement Decree.
[237] Article 13(5) and 13-4(3) CPPA.
[238] Article 7(2) CPPA.
[239] Article 7(2) CPPA and Article 5 CPPA Enforcement Decree.
[240] Article 9-2(3) CPPA. In accordance with Article 13-4 CPPA, this applies both to the collection of the content of communications and of communication confirmation data.
[241] Article 9-2(4) CPPA.
[242] Articles 13-4(2) and 9-2(6) CPPA.

This notification requirement however only applies to the collection of information where at least one of the parties is a Korean national. As a consequence, non-Korean nationals will only be notified when their communications with Korean nationals are collected. There is therefore no notification requirement when communications exclusively between non-Korean nationals are collected.

The content of any communications as well as communication confirmation data acquired through surveillance on the basis of the CPPA may only be used (1) for the investigation, prosecution or prevention of certain crimes, (2) for disciplinary proceedings, (3) for judicial proceedings where a party relating to the communication relies on them in a claim for damages or (4) on the basis of other laws.[243]

3.2.1.2. Collection of communication information by the police/prosecutors for national security purposes

The police/prosecutor may collect communication information (both the content of communications and communication confirmation data) for national security purposes under the same conditions as described in section 3.2.1.1. When acting in emergency situations[244], the applicable procedure is the one that was described earlier with respect to the collection of the content of communications for law enforcement purposes in emergency situations (i.e. Article 8 CPPA).

3.2.2. Collection of information on terrorist suspects

3.2.2.1. Legal basis

The Anti-Terrorism Act empowers the Director of the NIS to collect information on terrorist suspects.[245] "*Terrorist suspect*" is defined as a member of a terrorist group,[246] a person who has propagated a terrorist group (by promoting and disseminating ideas or tactics of a terrorist group), raised or contributed funds for terrorism[247], or engaged in other activities of preparing, conspiring, propagandizing, or instigating terrorism, or a person for whom there are good grounds to be suspected of having performed such activities.[248] As a general rule,

---

[243] Articles 5(1)-(2), 12 and 13-5 CPPA.

[244] That is, where the measure aims at an act of conspiracy that threatens national security and an emergency exists that makes it impossible to go through the ordinary approval procedure (Article 8(1) CPPA).

[245] Article 9 Anti-Terrorism Act.

[246] "*Terrorist group*" is defined as a group of terrorists designated by the United Nations (Article 2(2) Anti-Terrorism Act).

[247] "*Terrorism*" is defined by Article 2(1) Anti-Terrorism Act as conduct carried out for the purpose of impeding the exercise of the authority of the State, a local government or a foreign government (including local governments and international organisations), or for the purpose of causing it to conduct any affair which is not obligatory for it, or threatening the public. This includes (a) killing a person or posing a risk to a person's life by causing bodily injury or arresting, confining, kidnapping, or taking a person hostage; (b) certain types of conduct targeted at an aircraft (e.g. crashing, hijacking or damaging an aircraft in flight); (c) certain types of conduct related to a ship (e.g. seizing a ship or marine structure in operation, destroying a ship or marine structure in operation or inflicting damage thereon to a degree that endangers the safety thereof, including damaging the cargo loaded on a ship or marine structure in operation); (d) placing, detonating, or using in any other way a biochemical, explosive, or incendiary weapon or device with the intention to cause death, serious injury, or serious material damage or having such effect on certain types of vehicles or facilities (e.g. trains, trams, motor vehicles, public parks and stations, facilities to supply electricity, gas and telecommunications etc.); (e) certain types of conduct related to nuclear materials, radioactive materials, or nuclear facilities (e.g. harming human lives, bodies, or property, or otherwise disturbing public safety by destroying a nuclear reactor or wrongfully manipulating radioactive materials, etc.).

[248] Article 2(3) Anti-Terrorism Act.

any public official enforcing the Anti-Terrorism Act must respect the basic rights enshrined in the Korean Constitution.[249]

The Anti-Terrorism Act does not by itself set out specific powers, limitations and safeguards for the collection of information on terrorist suspects, but rather refers to the procedures in other statutes. First, on the basis of the Anti-Terrorism Act, the Director of the NIS may collect (1) information on the entry into and departure from the Republic of Korea, (2) information on financial transactions and (3) information on communications. Depending on the type of information sought, the relevant procedural requirements are provided in the Immigration Act and Customs Act, the ARUSFTI or the CPPA, respectively.[250] For the collection of information on the entry into and departure from Korea, the Anti-Terrorism Act refers to the procedures set out in the Immigration Act and the Customs Act. However, these acts at present do not provide for such powers. For the collection of communication information and financial transaction information, the Anti-Terrorism Act refers to the limitations and safeguards in the CPPA (which are further detailed below) and the ARUSFTI (which, as explained in section 2.1, is not relevant for the purpose of the assessment for the adequacy decision).

In addition, Article 9(3) of the Anti-Terrorism Act specifies that the Director of the NIS may request personal information or location information of a terrorist suspect from a personal information controller[251] or a location information provider.[252] This possibility is limited to requests for voluntary disclosure, to which personal information controllers and location information providers are not required to respond, and in any event may only do so in accordance with PIPA and the Location Information Act (see section 3.2.2.2 below).

3.2.2.2. Limitations and safeguards applying to voluntary disclosure under PIPA and the Location Information Act

Requests for voluntary cooperation under the Anti-Terrorism Act must be limited to information on terrorist suspects (see above section 3.2.2.1). Any such request from the NIS must comply with the principles of lawfulness, necessity and proportionality following from the Korean Constitution (Articles 12(1) and 37(2))[253] as well as the PIPA requirements for the collection of personal information (Article 3(1) PIPA, see above section 1.2). The NIS Act furthermore specifies that the NIS may not force any institution, organisation or individual to do anything they are not obligated to do, nor obstruct any person's exercise of rights, by abusing its official authority.[254]A violation of this prohibition may be subject to criminal sanctions.[255]

Personal information controllers and location information providers receiving requests from the NIS on the basis of the Anti-Terrorism Act are not required to comply. They may comply on a voluntary basis, but are only allowed to do so in accordance with PIPA and the Location Information Act. . As regards compliance with PIPA, the controller must in particular take

[249] Article 3(3) Anti-Terrorism Act.
[250] Article 9(1) Anti-Terrorism Act.
[251] As defined in Article 2 PIPA, i.e. a public institution, legal person, organization, individual, etc. that processes personal information directly or indirectly to operate personal information files for official or business purposes.
[252] As defined in Article 5 Act on the Protection, Use, etc. of Location Information (hereafter "Location Information Act"), i.e. anyone that has obtained permission from the Korea Communications Commission to engage in a location information business.
[253] See also Article 3(2) and (3) Anti-Terrorism Act.
[254] Article 11(1) NIS Act.
[255] Article 19 NIS Act.

into account the interests of the data subject and may not disclose the information if it would be likely to infringe unfairly on the interest of the individual or a third party.[256] In addition, in accordance with Notification No. 2021-1 on Supplementary rules for the interpretation and application of the Personal Information Protection Act, the concerned individual must be notified of the disclosure. In exceptional situations, such notification may be delayed, in particular if and for as long as the notification would jeopardise an ongoing criminal investigation or is likely to harm the life or body of another person, where those rights or interests are manifestly superior to the rights of the data subject.[257]

3.2.2.3. Limitations and safeguards under the CPPA

On the basis of the Anti-Terrorism Act, intelligence agencies may only collect communication information (both the content of communications and communication confirmation data) when necessary for counterterrorism activities, i.e. activities related to the prevention of and countermeasures against terrorism. The procedures of the CPPA described in section 3.2.1 apply to the collection of communication information for anti-terrorism purposes.

3.2.3. Voluntary disclosure by telecommunications business operators

On the basis of the TBA, telecommunications business operators may comply with a request to disclose "communications data" from an intelligence agency that intends to collect the information to prevent a threat to national security.[258] Any such request must comply with the principles of lawfulness, necessity and proportionality following from the Korean Constitution (Articles 12(1) and 37(2))[259] as well as the PIPA requirements for the collection of personal information (Article 3(1) PIPA, see above section 1.2). Moreover, the same limitations and safeguards as with respect to voluntary disclosures for law enforcement purposes apply (see section 2.2.3).[260]

A telecommunication business operators is not required to comply, but may do so on a voluntary basis and only in accordance with PIPA. In this respect, the same obligations, including as regards notification of the individual, apply to telecommunication business operators as when they receive requests from criminal law enforcement authorities, as explained in more detail in section 2.2.3.

3.3. Oversight

Different bodies oversee the activities of Korean intelligence agencies. The oversight of the Defense Security Support Command is carried out by the Ministry of National Defense, pursuant to the Ministry's Directive on Implementation of Internal Audit. The NIS is subject to oversight by the executive, the National Assembly and other independent bodies, as explained in more detail below.

3.3.1. The Human Rights Protection Officer

[256] Article 18(2) PIPA.

[257] Notification No. 2021-1 of the PIPC on Supplementary rules for the interpretation and application of the Personal Information Protection Act, Section III, 2, (iii).

[258] Article 83(3) TBA.

[259] See also Article 3(2) and (3) Anti-Terrorism Act.

[260] In particular, the request must be in writing and state the reasons for the request, as well as the link to the relevant user and the scope of requested information, and the telecommunications business provider must keep records and report to the Minister of Science and ICT twice per year.

When intelligence agencies collect information on terrorist suspects, the Anti-Terrorism Act provides for oversight by the Counterterrorism Commission and the Human Rights Protection Officer (hereafter "HRPO").[261]

The Counterterrorism Commission inter alia develops policies concerning counterterrorism activities and oversees the implementation of counterterrorism measures as well as the activities of different competent authorities in the area of counterterrorism.[262] The Commission is chaired by the Prime Minister and comprised of several ministers and heads of governmental agencies, including the Minister of Foreign Affairs, the Minister of Justice, the Minister of National Defense, the Minister of Interior and Safety, the Director of the NIS, the Commissioner General of the National Police Agency and the Chairman of the Financial Services Commission.[263] When conducting counterterrorism investigations and tracing terrorist suspects to collect information or materials necessary for counterterrorism activities, the Director of the NIS must report to the Chairperson of the Counterterrorism Commission (i.e. the Prime Minister).[264]

The Anti-Terrorism Act furthermore establishes the HRPO in order to protect the basic rights of individuals against infringements caused by counterterrorism activities.[265] The HRPO is appointed by the Chairperson of the Counterterrorism Commission among individuals that meet the qualifications listed in the Enforcement Decree of the Anti-Terrorism Act (i.e. anyone qualified as an attorney-at-law with at least ten years working experience, or with expert knowledge in the field of human rights and serving or having served (at least) as an associate professor for at least ten years, or having served as a higher public official in State agencies or local governments, or with at least ten years working experience in the field of human rights, e.g. in a non-governmental organisation).[266] The HRPO is appointed for two years (with the possibility for a renewed term) and may only be removed from office on specific, limited grounds and for good cause, e.g. when indicted in a criminal case related to his/her duties, when divulging confidential information, or because of long-term mental or physical incapacity.[267]

In terms of powers, the HRPO may issue recommendations for improving the protection of human rights by agencies involved in counterterrorism activities, and process civil petitions (see section 3.4.3).[268] Where the existence of an infringement of human rights in the performance of official duties can reasonably be established, the HRPO may recommend the head of the responsible agency to correct such violation.[269] In turn, the responsible agency must notify the HRPO of the action undertaken to implement such recommendation.[270] If an agency would fail to implement a recommendation of the HRPO, the matter would be elevated to the Commission, including its Chairperson, the Prime Minister. So far, there have been no cases where HRPO recommendations have not been implemented.

3.3.2. The National Assembly

[261] Article 7 Anti-Terrorism Act.
[262] Article 5(3) Anti-Terrorism Act.
[263] Article 3(1) Anti-Terrorism Act Enforcement Decree.
[264] Article 9(4) Anti-Terrorism Act.
[265] Article 7 Anti-Terrorism Act.
[266] Article 7(1) Anti-Terrorism Act Enforcement Decree.
[267] Article 7(3) Anti-Terrorism Act Enforcement Decree.
[268] Article 8(1) Anti-Terrorism Act Enforcement Decree.
[269] Article 9(1) Anti-Terrorism Act Enforcement Decree. The HRPO decides autonomously on the adoption of recommendations, but is required to report such recommendations to the Chairperson of the Counterterrorism Commission.
[270] Article 9(2) Anti-Terrorism Act Enforcement Decree.

As described in section 2.3.2, the National Assembly may investigate and inspect public authorities and in that context request the disclosure of documents and compel the appearance of witnesses. With respect to matters falling under the jurisdiction of the NIS, this parliamentary oversight is carried out by the Intelligence Committee of the National Assembly.[271] The Director of the NIS, who oversees the performance of duties by the agency, reports to the Intelligence Committee (as well as the President).[272] The Intelligence Committee itself may also request a report on a specific matter, to which the Director of the NIS is required to respond without delay.[273] (S)he may only refuse to reply to or testify before the Intelligence Committee with respect to state secrets concerning military, diplomatic or North Korea-related issues where public knowledge may have a serious impact on the national destiny.[274] In this case, the Intelligence Committee may request an explanation from the Prime Minister. If such an explanation is not submitted within seven days of making the request, the reply or testimony may no longer be refused.

If the National Assembly finds that there has been unlawful or improper activity, it may request that the relevant public authority takes corrective measures, including awarding compensation, taking disciplinary action, and improving its internal procedures.[275] Following such a request, the authority must act without delay and report the outcome to the National Assembly. Specific rules regarding parliamentary oversight exist with respect to the use of communication-restricting measures (i.e. the collection of the content of communications) under the CCPA.[276] As regards the latter, the National Assembly may ask the heads of intelligence agencies for a report on any specific communication-restricting measure. In addition, it may conduct on-the-spot inspections of wire-tapping equipment. Finally, intelligence agencies that have collected and operators that have disclosed content information for national security purposes have to report on such disclosure upon request from the National Assembly.

3.3.3. The Board of Audit and Inspection

The BAI carries out the same oversight functions with respect to intelligence agencies as in the area of criminal law enforcement (see section 2.3.2).[277]

3.3.4. The Personal Information Protection Commission

As regards data processing for national security purposes, including the collection stage, additional oversight is carried out by the PIPC. As explained in more detail in section 1.2, this includes the general principles and obligations set out in Articles 3, 58(4) PIPA as well as the exercise of individual rights guaranteed by Article 4 PIPA. Moreover, according to Article 7-8(3), (4) and Article 7-9(5) PIPA, the oversight of the PIPC also covers possible infringements of the rules contained in specific laws setting out the limitations and safeguards with respect to the collection of personal information, such as the CPPA, the Anti-Terrorism Act and the TBA. Given the requirements in Article 3(1) PIPA for the lawful and fair

---

[271] Articles 36 and 37(1)16 National Assembly Act.

[272] Article 18 NIS Act.

[273] Article 15(2) NIS Act.

[274] Article 17(2) NIS Act. "State secrets" are defined as "*the facts, goods or knowledge classified as state secrets, the access to which is permitted to a limited scope of persons and which shall not be disclosed to any other country or organization, in order to avoid any serious disadvantage to the national safety*", see Article 13(4) NIS Act.

[275] Article 16(2) Act on the Inspection and Investigation of State Administration.

[276] Article 15 CPPA.

[277] As is the case with respect to the Intelligence Committee of the National Assembly, the Director of the NIS may only refuse to reply to the BAI on matters that constitute state secrets and if public knowledge would have a serious impact on national security (Article 13(1) NIS Act).

collection of personal information, any infringement of those Acts constitutes a violation of PIPA. The PIPC thus has the power to investigate[278] violations of the laws governing access to data for national security purposes as well as the processing rules in PIPA, and issue advice for improvement, impose corrective measures, recommend disciplinary action and refer potential offences to the relevant investigative authorities.[279]

3.3.5. The National Human Rights Commission

Oversight by the NRHC applies in the same way to intelligence agencies as to other government authorities (see section 2.3.2).

3.4. Individual redress

3.4.1. Redress before the Human Rights Protection Officer

With respect to the collection of personal information in the context of counterterrorism activities, a specific redress avenue is provided by the HRPO, established under the Counterterrorism Commission. The HRPO handles civil petitions related to the infringement of human rights as a consequence of counterterrorism activities.[280] (S)he may recommend corrective action and the relevant agency must report to the Officer any measures taken to implement such recommendation. There is no standing requirement for individuals to lodge a complaint with the HRPO. As a consequence, a complaint will be processed by the HRPO even if the concerned individual cannot demonstrate an injury in fact at the admissibility stage.

3.4.2. Redress mechanisms available under PIPA

Individuals may exercise their rights of access, correction, deletion and suspension under PIPA with respect to personal information processed for national security purposes.[281] Requests to exercise these rights can be filed directly with the intelligence agency, or indirectly via the PIPC. The intelligence agency may delay, limit or deny the exercise of the right to the extent and for as long as necessary and proportionate to protect an important objective of public interest (e.g. to the extent that and for as long as granting the right would jeopardise an ongoing investigation or threaten national security), or where granting the right may cause damage to the life or body of a third party. Where the request is denied or restricted, the individual must be notified of the reasons without delay.

Moreover, in accordance with Article 58(4) PIPA (requirement to ensure the appropriate handling of individual grievances) and Article 4(5) PIPA (right to appropriate redress for any damage arising out of the processing of personal information, through a prompt and fair procedure), individuals have the right to obtain redress. This includes the right to report an alleged violation to the Privacy Call Centre operated by the Korea Internet and Security Agency and file a complaint with the PIPC.[282] These redress avenues are available both in case of possible infringements of the rules contained in specific laws setting out the limitations and safeguards with respect to the collection of personal information for national security purposes and of PIPA. As explained in Notification No. 2021-1, an EU individual may submit a complaint to the PIPC through his/her national data protection authority . In this case, the PIPC will notify the individual via the national data protection authority once the investigation is concluded (including, where applicable, with information about the

[278] Article 63 PIPA.
[279] Articles 61(2), 65(1), 65(2) and 64(4) PIPA.
[280] Article 8(1) lit 2 Anti-Terrorism Act Enforcement Decree.
[281] Article 3(5) and Article 4(1), (3) and (4) PIPA.
[282] Articles 62 and 63(2) PIPA.

corrective measures imposed). Decisions or inaction by the PIPC can be further appealed before the Korean courts under the Administrative Litigation Act.

3.4.3. Redress before the National Human Rights Commission

The possibility to obtain individual redress before the NHRC applies in the same way to intelligence agencies as to other government authorities (see section 2.4.2).

3.4.4. Judicial redress

As is the case with respect to the activities of criminal law enforcement authorities, individuals may obtain judicial redress against intelligences agencies with respect to violations of the abovementioned limitations and safeguards through different avenues.

First, individuals may obtain compensation for damages under the State Compensation Act. For instance, in one case, compensation was granted with respect to unlawful surveillance by the Defense Support Command (the predecessor of the Defense Security Support Command).[283]

Second, the Administrative Litigation Act allows individuals to challenge dispositions and omissions by administrative agencies, including intelligence agencies.[284]

Finally, individuals may lodge a constitutional complaint with the Constitutional Court against measures taken by intelligence agencies on the basis of the Constitutional Court Act.

[283] Supreme Court Decision No. 96Da42789, 24 July 1998.
[284] Articles 3 and 4 Administrative Litigation Act.