EUROPEAN
COMMISSION

Brussels, 23.7.2026
SWD(2026) 231 final

COMMISSION STAFF WORKING DOCUMENT

Accompanying the document

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

on the first review of the functioning of the adequacy decision for the Republic of Korea

{COM(2026) 384 final}

1. INTRODUCTION

This document presents the findings of the Commission's services regarding the first evaluation of the Commission's implementing decision of 17 December 2021 pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data by the Republic of Korea under the Personal Information Protection Act (the adequacy decision or the decision)[1]. The findings are based on information gathered in the review meeting on 17 October 2025, as well as its preparation and follow-up. Among others, it relies on input from the Korean authorities, relevant stakeholders and publicly available material.

2. THE ADEQUACY DECISION

In the adequacy decision, the Commission found that, for the purposes of Article 45 of Regulation (EU) 2016/679 (GDPR), the Republic of Korea ensures an adequate level of protection for personal data transferred from the European Union (Union or EU). Consequently, data transfers from the EU to the Republic of Korea that fall within the scope of the decision are permitted under EU data protection law without additional requirements[2].

The adequacy decision covers the Personal Information Protection Act (PIPA)[3] as complemented by the additional safeguards set out in Annex I to that adequacy decision (Supplementary Rules)[4], together with the official representations, assurances and commitments contained in Annex II to the adequacy decision. The latter concern the limitations and safeguards as regards access by Korean public authorities to the personal data transferred.

3. THE FIRST REVIEW – BACKGROUND, PREPARATION AND CONSULTATION OF STAKEHOLDERS

To regularly verify that the findings in the Commission's adequacy decision are still factually and legally justified, the decision provides for its periodic review based on all available information[5]. In this regard, it is important to note that, since the adoption of the adequacy decision, the Republic of Korea has amended the PIPA on two occasions: in March 2023 and in April 2025[6]. Both amendments as well as the amendments of the related Enforcement Decree[7] are assessed in this

[1] Commission Implementing Decision (EU) 2022/254 of 17 December 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 (notified under document C(2021) 9316) (Text with EEA relevance), C/2021/9316, OJ L 44, 24.2.2022, pp. 1–90.
[2] See Article 45 GDPR and recital 5 of the decision.
[3] PIPA provides the general legal framework for data protection in the Republic of Korea.
[4] Specific rules put in place by Korea to bridge certain relevant differences between the PIPA and the GDPR specified in Annex I to the adequacy decision (Notification No 2021-5).
[5] Article 45(3) Regulation (EU) 2016/679 provides that a periodic review must take place 'at least every four years'. See recital 227 and Article 3(4) of the Decision.
[6] Respective entry into force in September 2023 and October 2025.
[7] See section 4.1.1.4.

report. The Commission's review, which covers all aspects of the adequacy decision, has put particular emphasis on assessing the impact of these important legal developments.

As required by recital 220 of the adequacy decision, the first review has focused on the safeguards existing for onward transfers[8], relevant case law, and the rules on processing pseudonymised data for statistics, research, and archiving. The review has also evaluated the effectiveness of individual rights, government access limitations, oversight, enforcement, and the cooperation between the Korean data protection authority, the Personal Information Protection Commission (PIPC), and EU data protection authorities on complaints from individuals.

To prepare the first review, the Commission services gathered information from the Korean authorities on the functioning of the Decision, in particular the implementation of the Supplementary Rules, protections for onward transfers, the effectiveness of individual rights, and the application of exceptions to these rights. Furthermore, the Commission services evaluated developments in the area of oversight and enforcement, in particular with respect to the PIPA, law enforcement and national security access to personal data, and cooperation between the PIPC and EU data protection authorities. The Commission services did not receive any information from the Member States pursuant to Article 2 and Article 3(2)-(3) of the adequacy decision.

The review meeting took place on 17 October 2025. On the Korean side, representatives from the PIPC and from the Korea Internet and Security Agency (KISA) participated in the meeting. Moreover, in the preparation of the review meeting, the PIPC gathered information from other relevant Korean authorities.

The EU delegation included four representatives designated by the European Data Protection Board (EDPB), alongside members of the European Commission services[9]. In preparation and further to the review meeting, the Commission and the PIPC had several exchanges to follow up on specific points.

Finally, the four EDPB representatives have been consulted on this document and provided feedback on the findings.

4. THE FIRST REVIEW – FINDINGS

4.1. THE DATA PROTECTION FRAMEWORK IN THE REPUBLIC OF KOREA

The following sections present the Commission services' findings with respect to the "commercial aspects" of the adequacy decision (i.e. the data protection rules applicable to public and private controllers and processors). The Commission services review of these aspects has in particular focused on the impact of the 2023 and 2025 PIPA amendments relating to the rights and safeguards afforded to EU individuals (whose personal data is transferred from the EU) under Korean law

[8] See section 2.3.9 of the adequacy decision, referring to Data transferred from the EU to the Republic of Korea that is transferred again to a third country.

[9] The EDPB team consisted of representatives from the data protection supervisory authorities of Italy, France, Finland and Germany.

(section 4.1.1). In addition, the Commission services have assessed the relevant developments in the Korean legal framework on oversight and enforcement since the adoption of the adequacy decision (section 4.1.2). Finally, the Commission services have evaluated whether the Supplementary Rules – which were enacted to offer enhanced protection to EU individuals when their personal data is transferred to Korea based on the adequacy decision – are functioning in the way that is envisaged in the decision, and whether the recent amendments to PIPA have created overlaps that have made certain Supplementary Rules redundant (section 4.1.3).

4.1.1. Relevant developments in the Korean legal framework

The 2023 PIPA amendment has significantly strengthened the level of protection guaranteed by the PIPA in several important areas, such as with respect to its scope, the rights of data subjects, and the restrictions on international transfers of personal data, and in this way also further increased the degree of convergence between the EU and the Korean data protection systems.

4.1.1.1. Scope, principles and key concepts

At the time of the adoption of the Commission adequacy decision, the PIPA already had a broad scope of application, so that the adequacy decision covered both the public and private sectors. Since the 2023 amendments, **PIPA's scope of application** now **extends to two specific sectors** that were previously excluded. The exceptions that previously applied to personal data collected under the Statistics Act and processed by public institutions, as well as to personal data processed temporarily where it is urgently necessary for the public safety, security and public health, have now been both removed[10]. Accordingly, the provisions in the PIPA now apply to both activities in full[11].

Moreover, at the time of adoption of the adequacy decision, the PIPA contained a chapter with specific provisions that were applicable only to the processing of personal data of 'users' by 'providers of information and communication services'[12]. With the amendments to the PIPA in 2023, the chapter with those special rules has been deleted and such types of processing situations are now covered by the general rules of PIPA. Some of the rights that were previously guaranteed only for this specific situation have now been included in the general PIPA rules.

The amendments to the PIPA have also further developed and clarified and certain principles relating to the processing of personal information[13]. For instance, as regards the **principle of lawfulness,** there have been some changes to the existing legal bases for processing. For instance, Article 15(1)(4) PIPA, which at the time of the adoption of the adequacy decision allowed processing when unavoidable to execute and perform a contract with the data subject[14], has been revised to broaden the legal basis for collecting and using personal data in relation to contract

[10] See recital 27 and 29 of the adequacy decision.
[11] The PIPC explained that, while the PIPA provisions apply in full, the legal bases for processing in these cases are provided under relevant sector-specific laws such as the Statistics Act, the Infectious Disease Control and Prevention Act, and the Framework Act on Disaster and Safety Management.
[12] See section 2.2.4 of the adequacy decision referring to Chapter VI of PIPA.
[13] PIPA uses more frequently the term "personal information". As it was explained in Section 2.2.1 of the adequacy decision, it is equivalent to the term "personal data".
[14] See recital 35 of the adequacy decision.

performance. Following the amendment, the requirement that the processing be "unavoidable" has been removed, and the processing of personal data at the request of the data subject is now permitted when necessary to take measures at the request of a data subject in the course of concluding and performing a contract[15].

In addition, Article 15(1)(7) PIPA now also allows processing "*where it is urgently necessary for the public safety and security, public health, etc*.". According to the PIPC, this change is linked to the fact that the PIPA now applies in full to processing for emergency situations, for the protection of public safety and health, or for other essential public interests[16].

Finally, Article 22 PIPA, which describes the methods of obtaining consent, has been revised and is now clearer. The situations requiring separate consent have been clearly spelled out[17] and a new article in the PIPA clarifies that consent for processing the personal data of children must be obtained from their legal representative[18].

With regard to the **principle of transparency**, the 2023 PIPA amendments have established further safeguards to mitigate potential risks of data subjects inadvertently revealing sensitive information whilst utilising services. Pursuant to the revised provision, if a data controller believes there is a risk of privacy infringement - for instance, when a data subject voluntarily inputs sensitive information in a way that may render it publicly visible during the use of goods or services - the controller must warn the data subject prior to the disclosure of such information. This warning should explicitly inform the data subject that the sensitive information may become publicly accessible, and that they have the option to opt out or choose non-disclosure settings if they prefer the information to remain private[19].

Specific transparency requirements have also been introduced with respect to children. The PIPA now requires State and local governments to specifically take into account the rights of children under 14 years, including to ensure that they understand the impact of data processing[20]. Moreover, the obligation to provide children with clear and easy-to-understand explanations regarding the processing of their personal data, which previously applied only to information and communications service providers, has been extended to all controllers[21].

With regard to the **principle of accountability**, the amendments of the PIPA in 2025 concerned the need to appoint a domestic agent in Korea. Under the revised Article 31-2 PIPA, where a

[15] Article 6(1)(b) GDPR does not require that processing is "unavoidable" and rather refers to the "necessity of processing for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract".
[16] The PIPC has explained that the term "etc." indicates that other situations of a similar nature are also included. It functions similarly to "such as" or "including but not limited to" in English.
[17] Article 22 PIPA.
[18] Article 22-2 (1) PIPA.
[19] However, an exemption is applicable in situations where the inherent purpose of the service needs public disclosure and for interactive communication, such as public noticeboards or social networking services (SNS), and it is reasonable to presume that the data subject is aware of the fact that the information they provide will be publicly disseminated. In these circumstances, the requirement to show an explicit notification regarding public disclosure may be waived. The PIPC has published guidelines that explain with examples how this can be implemented.
[20] Article 5(3) PIPA.
[21] Article 22-2 (3) PIPA. The previous obligation was in Article 39-3(5) PIPA.

personal information controller has established a domestic corporation or exercises substantial influence over the management, governance, or operations of a domestic company[22], the controller is now required to appoint such an entity as its domestic agent. While this obligation existed previously in Article 39-11 PIPA, it was limited to information and communications service providers. As the Commission explained in recitals 24 and 25 of the adequacy decision, such provisions were previously applicable in very limited situations, while now this requirement is of general nature. The scope of application was subsequently expanded to all controllers through the 2023 amendment, while the 2025 amendment introduced additional requirements regarding the designation of a domestic agent.

The changes introduced in the PIPA in 2023 also concerned the concept of **pseudonymised data**. The restrictions that existed for processing pseudonymised information and that were described in the adequacy decision have been further tightened[23]. First, Article 28-7 PIPA has been amended to further codify that certain exceptions on transparency and individual rights apply exclusively to pseudonymised data used for statistical, scientific research, or public archiving purposes[24]. This is further developed by the guidelines on processing pseudonymised information of the PIPC[25], which explain that storing personal information in a pseudonymised form in a situation where the purpose of processing has not been established cannot be considered valid processing of pseudonymised information. Furthermore, those guidelines also clarify that when a personal information controller receives a request to suspend pseudonymisation from a data subject, the controller must immediately suspend all or part of the processing of the data subject's personal information. If the personal information of the subject has already been pseudonymised, the request to cease the use of the pseudonymised data does not apply.

Second, after the amendments introduced to the PIPA in 2023, pseudonymised data is now also subject to Article 21 PIPA, which establishes the obligation to destroy personal information once it becomes unnecessary in consideration of the expiry of the retention period, or the attainment of the established purpose. Such processing period might be separately determined for pseudonymised data in consideration of the specific purpose of processing[26]. At the time of the adequacy decision, the respective obligation to destroy the data did not apply when pseudonymised data was processed for statistical purposes, scientific research or archiving in the public interest[27]. To ensure the principle of limited data retention also in this case, Notification 2021-5 was

[22] This refers to controllers with no address or place of business in the Republic of Korea.
[23] See in this regard recitals 42 to 48 of the adequacy decision. As at the time of the adequacy decision, 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 and archiving in the public interest, subject to specific safeguards. PIPA imposes pseudonymisation 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).
[24] The Article now reads: Articles 20, 20-2,27, 34 (1), 35, 352, 36, and 37 shall not apply to pseudonymised information processed under Article 28-2 or 28-3 PIPA.
[25] PIPC Pseudonymised Information Processing Guidelines.
[26] Article 28-4 (2) PIPA.
[27] See recital 60 of the adequacy decision.

introduced to require 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[28].

The new PIPA provisions also ensure further transparency about the processing of pseudonymised data. In this regard, since the 2023 amendments to the PIPA, the privacy policy must also inform about the fact that pseudonymised data is being processed[29].

These changes have been also accompanied by specific guidelines published by the PIPC in 2024[30]. The guidelines explain the principles for safe pseudonymisation and also provide examples across sectors such as healthcare, transportation, and chatbot services.

The rules regarding the processing of pseudonymised data have also been further clarified through case law and developments in the enforcement practice. For instance, since the adoption of the adequacy decision, the Supreme court has interpreted these rules, finding that, even if information is used for statistical purposes or shared with third parties without the data subject's consent, it still constitutes personal data under the PIPA if there is a reasonable possibility of re-identification[31]. If such reasonable risk of re-identification exists, data must be considered personal data, and the full protection of the PIPA continues to apply. Such possibilities of re-identification would be considered in light of encryption or other appropriate de-identification measures. Moreover, on 18 July 2025 the Supreme Court issued a judgment clarifying the scope of the right to request suspension of processing under Article 37 PIPA[32]. In that matter, the Court held that the pseudonymisation process is a distinct protective measure under the PIPA and is not subject to the right of suspension under Article 37PIPA[33].

4.1.1.2.Strengthening of data subject rights

Since the adoption of the adequacy decision, data subject rights have been strengthened under Korean law.

First, the PIPA now contains a general **right to withdraw consent**. Under the new version of Article 37 (1) PIPA, this right is recognised in addition to the existing right to request the suspension of processing of personal data.

When data subjects withdraw their consent, the personal information controller must take appropriate actions, such as halting processing or deleting the data, as if the data subject had requested a suspension of processing. In addition, if the controller rejects the request - whether to suspend processing or to withdraw consent - based on a specific legal provision or another valid reason, it is obliged to promptly inform the data subject of the reasons for the refusal.

[28] Section 4 of Notification 2021-5.
[29] Article 30(1)4-2 PIPA.
[30] PIPC Pseudonymised Information Processing Guidelines.
[31] Supreme Court 2019Da242045 and Supreme Court, 2019Da242052.
[32] Article 37 PIPA reads: A data subject may request the relevant personal information controller to suspend the processing of his or her personal information or may withdraw his or her consent to personal information processing. In such cases, if the personal information controller is a public institution, the data subject may request the institution to suspend the processing of his or her personal information contained in the personal information files to be registered pursuant to Article 32 or may withdraw his or her consent to personal information processing.
[33] See Supreme Court, 2024Da210554.

Moreover, the PIPA now foresees that data subjects have a right to object to **automated-decision making** where such decisions significantly affect their rights or obligations, including their life, body or property, and to obtain explanations for such decisions, including those based on artificial intelligence. In this regard, Article 37-2 PIPA provides first a right to object to a decision or to request an explanation about a decision taken solely on the basis of automated processing of personal data. In that case, the controller must follow the request and either not apply the automated decision unless there are compelling reasons[34], or take necessary measures, such as re-processing through human involvement, and provide explanations. In addition, controllers are required to disclose the standards, procedures, and methods of personal data processing used in automated decision-making in a manner that is easily understandable to data subjects[35]. This ensures that individuals are adequately informed and empowered to exercise their rights effectively.

Moreover, in September 2024, the PIPC issued a guide on the rights of data subjects concerning automated decision making[36]. The guide provides detailed explanations and specific examples of when a decision is considered "automated" and the actions that a controller must take when such decisions occur.

While a specific type of automated administrative dispositions is excluded from the protections of Article 37-2 (1) PIPA[37], according to the explanations provided by the PIPC in the guidelines on automated decision making, such type of automated decisions is limited to situations where there is no discretion on the side of the public administration. Moreover, data subjects are entitled to existing legal remedies under the Administrative Procedures Act or the Administrative Litigation Act also for those decisions. During the review meeting, the PIPC confirmed that such legal remedies are also available to EEA data subjects. Article 37-2 (1) PIPA also excludes from its protection situations where the data subject has provided consent, where processing is carried out on the basis of a legal statute, or where actions must be taken at the data subject's request during the creation or execution of a contract[38]. The guidelines on automated processing contain clear examples for when those exceptions can be relied on, and how the data subject must be informed about them.

The 2023 legislative reform also introduced a **general right to data portability** in Article 35-2 PIPA. According to that provision, a data subject may request specific personal information controllers to transmit the personal data either to the data subject directly or to a third

[34] According to the Guidelines on automated decision making, when determining whether there is a justified reason to refuse action in response to a request by a data subject, the following aspects have to be assessed: i) the existence of legal obligations, including an indispensability to comply with specific statutory provisions (e.g. in the prevention of fraud), ii) potential harm to the life or body of another person if the refusal is granted, iii) potential unfair infringement to a third person's property or interests, and iv) whether rejecting the automation would make fulfilling a contract impractical.
[35] Article 37-2 (2) and (4) PIPA.
[36] PIPC Guide to Data Subjects' Rights Regarding Automated Decision-Making.
[37] In particular, automated administrative dispositions under Article 20 of the Framework Act on Administrative Regulations. In those dispositions, the administration does not exercise any discretion. Other automated decisions that do not fall under this narrow administrative exception continue to be subject to the protections of Article 37-2 PIPA.
[38] Article 37-2 (1) PIPA with reference to Article 15 (1) 1, 2, and 4 PIPA.

party designated by the data subject. Korea has established a specific platform called MyData for that purpose, which provides technical support for exercising the data portability right.

4.1.1.3. Strengthened rules on transfers of personal data outside of Korea

The 2023 reform of the PIPA introduced significant changes also to the rules for transfers of personal data outside of the Republic of Korea, ensuring further alignment with the rules in Chapter V of GDPR. The PIPA contains a new section on cross-border data transfers rules which provides different instruments that can be used for such transfers[39]. As a general principle, Article 28-8 PIPA now explicitly provides that no transfer of personal information by a personal information controller is allowed unless one of the specific transfer bases spelled out in that Article is used.

In terms of transfer bases, personal data may first be transferred outside of the Republic of Korea on the basis of "separate consent"[40]. As explained by the PIPC, the objective of requiring "separate consent" under Article 28-8(1)(1) PIPA is to ensure that the data subject clearly understands that the purpose of the consent is distinct from the consent obtained for the initial collection or use. Controllers are required to inform the data subjects in advance when obtaining such separate consent, in particular about the details of the data to be transferred, the country where that data is going to be transferred, the name of the recipient, the purpose of the transfer and the method and procedure for objecting to such transfer[41]. Moreover, where any of the information previously provided to the data subject in relation to the transfer has changed, the controller must notify the data subject of such changes and obtain their consent once again[42].

Second, personal data may be transferred outside of the Republic of Korea on the basis of special provisions in a statute or treaty to which the Republic of Korea is party to.

Third, data may be transferred where entrustment or storage of personal data is necessary for the signing or implementation of a contract with the data subject if the individual is notified about specific elements of the transfer, in particular the country to which the personal information is transferred, the transfer date, and the transfer method.

Fourth, a transfer is also possible based on a certification as prescribed by the PIPC and following the adoption of specific measures to ensure that information is dealt with safely in the third country and that data subjects have the possibility to exercise their rights[43]. The Republic of Korea has now developed a certification system (Information Security Management System–Personal Information, "ISMS-P") and the PIPC has established detailed regulations to further develop it[44]. The certification assesses the establishment and operation of internal management systems, the existence of technical, administrative and physical safeguards and compliance throughout the data processing lifecycle.

[39] Section IV as part of Chapter III. See in particular Articles 28-8, 28-9, 28-10 and 28-11 PIPA.
[40] Article 28-8 (1) subparagraph 1 PIPA.
[41] Article 28-8(2) PIPA.
[42] Article 28-8(3) PIPA.
[43] See also Article 32-2 PIPA.
[44] See the notice on Notice on Information Protection and Personal Information Protection Management System Certification, etc. [Effective July 24, 2024].

The PIPC has clarified that it has not recognised the APEC Cross Border Privacy Rules (CBPR) or Global CBPR as valid certification systems under Article 28-8(1)(4) PIPA, despite being a participating economy in both[45]. The PIPC has explained that in the Republic of Korea, the CBPR system is operated as a privacy trustmark, intended to help domestic businesses demonstrate an appropriate level of privacy protection when entering overseas markets without them being able to rely on CBPR certification as a tool for transfers to third countries. In this respect, as the Commission has highlighted on other occasions, the protections offered by the CBPR systems do not result from an arrangement binding the exporter and the importer in the context of their bilateral relationship and are insufficient[46]. The PIPC has confirmed through the review discussions that CBPR certification does not constitute a valid transfer mechanism under the PIPA. It also plans to publish and make available on its website guidelines explaining specific requirements and interpretations regarding cross-border data transfers, including this point. Accordingly, in case the PIPC were to consider CBPR as a valid transfer tool, this situation could affect the adequacy finding and would have to be remedied to continue ensuring safe data flows from the EEA. The Commission will continue to monitor closely developments in this area.

Finally, a transfer to a third country may also be based on an equivalence recognition adopted by the PIPC. Equivalence recognitions under the PIPA have similar effects to adequacy decisions under the GDPR and data may flow freely to the third country found equivalent without any additional safeguards. For that purpose, the PIPC assesses whether a foreign country or international organisation ensures a level of data protection that is equivalent to the one provided in Korea by examining its alignment with data protection principles, protection of data subject rights, presence of an independent supervisory authority, effectiveness of redress mechanisms, and potential for cooperation with the PIPC.

So far, the only equivalence recognition adopted by the PIPC concerns the European Union. It entered into force on 16 September 2025, covers both the public and the private sectors, and extends to the entire EEA[47].

Importantly, under the reformed regime, the PIPC retains the power to order a controller to suspend transfers of personal data in specific circumstances. It may do so in cases of non-compliance with the underlying consent, certification system or equivalence recognition relied on [48]. In other words, the PIPC monitors developments in third countries and international organisations and can take action if the conditions in the third country or jurisdiction no longer guarantee adequate protection for data transferred from Korea. Moreover, the protection ensured by Article 28-8 and Article 28-9 PIPA also has to be ensured in case of onward transfers, as the receiving entity in the third

[45] Korea implemented the APEC CBPR(Cross-Border Privacy Rules) system in 2022.
[46] See in this regard the Staff Working Document published following the review of the adequacy decision in Japan, SWD(2023) 75 final: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023SC0075.
[47] See Joint Press Statement of 16 September 2025 by Commissioner Michael McGrath and former Chairperson Haksoo Ko on the entry into force of the Korean adequacy decision on the EU.
[48] Article 28-9 PIPA.

country may only onward transfer the personal data if the requirements of the PIPA transfer regime are met[49].

As regards future plans for transfers, the PIPC explained during the review meeting that it is exploring to also allow cross-border transfers of personal data based on Standard Contractual Clauses (SCCs) or Binding Corporate Rules.

Based on the EU's positive experience with model clauses, the Commission believes that the development of such clauses could further strengthen the safeguards for (onward) transfers in transfer scenarios where the company processing information in the Republic of Korea and the third-country recipient intend to frame their transfer by together implementing measures providing a level of protection equivalent to the PIPA. For this reason, and given the growing importance of model clauses and their potential as a global tool for data transfers – as recognised for instance by ASEAN[50], the OECD [51], the G7[52] and the Ibero-American Network of data protection authorities [53]– the Commission would be interested in future cooperation with the Republic of Korea in the development of such clauses.

Finally, while the Republic of Korea has concluded digital agreements with certain third countries, including Singapore, New Zealand and Chile (Digital Economy Partnership Agreement, DEPA) the respective agreements do not affect the regime for international personal data transfers, that continue to be governed by Article 28-8 PIPA.

4.1.1.4. Changes to other relevant laws and decrees

As explained in the adequacy decision, 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[54]. Since the adoption of the adequacy decision, the CIA has been amended on two occasions[55], however the rules on how credit information must be processed have not been substantially revised[56]. Moreover, as explained in the adequacy decision, some PIPA provisions are further developed by PIPA's Enforcement Decree[57], which has been amended three times since 2021. The first amendment of September 2023 aligned the Enforcement Decree with relevant changes to the PIPA, established

[49] Article 28-11 PIPA. According to the provision: Where a person who has received personal information pursuant to the provision to the main clause of Article 28-8(1) further transfers such personal information to a third country, Articles 28-8 and 28-9 shall apply mutatis mutandis.
[50] See the ASEAN Model Contractual Clauses for Cross Border Data Flows (MCCs).
[51] See OECD Going Digital Toolkit, Interoperability of privacy and data protection frameworks, , p. 18.
[52] For instance, see Roundtable of G7 Data Protection and Privacy Authorities 2024 - G7 DPAs' Communiqué Privacy in the age of data, para 15.
[53] Implementation Guide to the Model Contractual Clauses for international data transfers.
[54] Credit information in this context was referred to as: "*information that is necessary to determine the creditworthiness of parties to financial or commercial transactions*".
[55] Korean Credit Information Use and Protection Act..
[56] The amendments concern Article 15(2) and Article 20(4) CIA. Article 15(2) CIA was changed to introduce a reference to processing when it is "*urgently necessary for the public safety and security, public health, etc.*" Article 20(4) CIA was also changed to reflect structural changes to PIPA.
[57] Presidential Decree No. 30892 of 4 August 2020.

thresholds for notification obligations, further specified the conditions for cross-border transfers[58], developed methods for parental consent verification[59] and introduced safety requirements for public institutions operating personal data systems of a specific size[60]. In March 2024, the Enforcement Decree was further amended to authorize the PIPC to conduct evaluations of the protection of personal data in public institutions[61] and to establish methods and procedures concerning automated-decision making[62]. Moreover, following the amendments introduced in 2025, the right to data portability and the use of the MyData platform were further developed[63].

4.1.2. Oversight and enforcement by PIPC

The PIPC continues to be the independent data protection authority in charge of enforcement of the PIPA in the Republic of Korea. In 2026 PIPC was composed of 1 Secretariat, 5 Bureaus, and 18 Divisions, with a total of 195 staff members. Moreover, it also had a dedicated MyData Task Force, consisting of one unit, three teams, and 15 staff members[64]. PIPC's yearly budget amounted to almost 42 million EUR[65].

Through the amendments of the PIPA in 2023, the role of the PIPC as a supervisory authority has been further strengthened, as its powers to adopt corrective measures, conduct inspections, and to impose fines have been reinforced as has its role in ensuring accountability by controllers.

More specifically, the provision in the PIPA giving the PIPC the power to adopt corrective measures has been amended to clarify that the authority may adopt such measures for any violation of the law[66]. Previous references to the risk of damage as a condition for such measures have been deleted, bringing further clarity to the legal framework and ensuring effective enforcement.

Furthermore, the PIPC has obtained the power to conduct inspections in cases where the controller is highly likely to have a committed a data breach and there is a need for such inspection[67]. The new provision allows the PIPC to inspect controllers even if the specific inspection conditions of Article 63(1) PIPA are not fulfilled[68].

As regards fines, the provisions on sanctions with strong criminal law nature have been further expanded. For instance, there are now penalty provisions of imprisonment and fines for persons

[58] Chapter IV-3 Cross Border Transfer of Personal Information of the Enforcement Decree.
[59] Article 17-2 Enforcement Decree.
[60] Articles 15-2 and 15-3 Enforcement Decree.
[61] Article 13-2 Enforcement Decree.
[62] Article 44-2 Enforcement Decree and Article 44-3 Enforcement Decree.
[63] Articles 42-3 to 42-16 Enforcement Decree.
[64] See section 4.1.1.2 for information on MyData.
[65] KRW 72.9 billion.
[66] Article 64 (1) PIPA now reads: The Protection Commission may order a person who violates this Act (excluding central administrative agencies, local governments, the National Assembly, the Court, the Constitutional Court, and the National Election Commission) to take the following measures: To suspend personal information breach; To temporarily suspend personal information processing; Other measures necessary to protect personal information and to prevent personal information infringement.
[67] Article 63-2 PIPA. Article 63(1) PIPA continues to be in force and gives the PIPC the power to conduct inspections when a violation of the act is found or suspected, where any violation of the act is reported or a complaint thereon is received or in cases where it is necessary to protect the personal information of data subjects.
[68] Article 63-2 PIPA.

that collect personal data of a child under 14 years of age without the consent of the child's legal representative, and for persons that consolidate pseudonymised information without the approval of the PIPC[69].

Furthermore, the regime for the imposition of administrative fines has been further strengthened by adding infringements that could potentially be subject to such type of sanctions[70]. For instance, administrative fines are now foreseen also for breaches of the notification duty under Article 20 PIPA, for failure to take measures to ensure the protection of data, or for failure to communicate to the data subject the possibility that sensitive data will be disclosed[71]. Moreover, the broader powers for inspections described in this section have also been combined with corresponding administrative fines in case of failure to submit materials or obstructions[72]. Importantly, the PIPC retains a margin of appreciation for reducing or exempting fines in consideration of the gravity of the infringement, its effects and the size of the controller[73].

Finally, the PIPC's role in improving accountability has been reinforced. The PIPC conducts annual evaluations of compliance by public authorities with PIPA, rewards excellence and makes recommendations to improve the protection of personal data[74]. Moreover, the PIPC now has the power to evaluate privacy policies and make recommendations[75], and to designate an institution to conduct privacy impact assessments[76]. In cases of serious personal data breaches resulting from violations of the PIPA, the authority to supervise such matters has now been consolidated under the PIPC. Furthermore, the PIPC may request cooperation from relevant administrative authorities for prompt and effective measures[77].

Since the adoption of the adequacy decision, the PIPC has been actively enforcing the PIPA provisions. In particular, on 14 September 2022, the PIPC issued corrective orders and administrative fines to Google and Meta for illegally collecting and using users' behavioural data, including tracking information across sites and apps, without proper consent for targeted advertising. The fines imposed on both companies totalled more than 57 million EUR[78]. The Seoul administrative court dismissed on 23 January 2025 the claims filed by Google and Meta against the decision[79].

In a decision of 8 February 2023, the PIPC issued corrective orders and levied an administrative fine on Meta for requiring users to provide behavioural data in order to use Facebook and Instagram services. This behavioural data, gathered from third-party websites and apps, was

[69] Article 71(3) and 71(6) PIPA respectively. Recitals 47 and 48 of the adequacy decision assess the restrictions on combining pseudonymised information (Article 28-3 PIPA).
[70] Article 75 PIPA.
[71] Article 75(2) (2), (5) or (6) PIPA respectively.
[72] Article 75(2)(25) and (26) PIPA.
[73] Article 75 (5) PIPA.
[74] Article 11-2 (4) PIPA.
[75] Article 30-2 PIPA.
[76] Article 33(2) PIPA. Article 36 of the Enforcement Decree further develops this provision.
[77] Article 64(2) PIPA. Administrative authorities used to have this authority in the past.
[78] Google: KRW 69.2 billion and Meta: KRW 30.8 billion.
[79] https://www.moj.go.kr/bbs/moj_eng/49/477160/download.do. See references Seoul Administrative Court, 2023GuHap55191 and Seoul Administrative Court, 2023GuHap54259. Both judgments are currently under appeal.

considered unnecessary for the main functions of those services, which are socializing and communicating with other people. In addition, the PIPC also found that Meta infringed the PIPA by refusing to provide services to customers who did not agree to Meta's collection of data from third party sites[80].

The PIPC enforcement activity also extends to international data transfers. In this regard, in early 2025 the authority investigated several conducts of DeepSeek in relation to its AI chatbot. The conducts assessed by the authority included unlawful cross-border transfers of personal data to overseas entities located in China and the United States without a valid legal basis, the use of prompt inputs for AI development and training without providing users with an option to opt out, the transmission of prompt input information to third parties and the omission of essential details regarding data destruction procedures and methods in its privacy policy[81]. The PIPC proposed that DeepSeek temporarily discontinue its chatbot service until completion of the necessary updates. DeepSeek agreed with the recommendation and took its application off the Apple App Store and Google Play on 15 February 2025. On 23 April 2025 the authority adopted a recommendation addressed to DeepSeek to correct and remedy its conduct with regard to the company's AI chatbot. Following the investigation, the PIPC asked DeepSeek to rely on valid legal bases for cross-border data transfers, destroy the data transferred abroad, make its privacy policy available in Korean and include a domestic agent. DeepSeek implemented the recommendations by the PIPC and is again active in the Republic of Korea.

Moreover, PIPC imposed sanctions on AliExpress and Temu for transfers of personal data outside of the country[82].

The enforcement of the rules on cybersecurity and of data breaches have also been high on the agenda of the PIPC. On 28 August 2025, the authority imposed a fine of more than 77 million EUR on SK Telecom for a personal data leak involving 23 million users. The fine was the highest ever imposed by the authority[83].

PIPC has also been active enforcing the rules regarding pseudonymised data. In April 2024, it imposed administrative fines and issued recommendations for improvement against two public institutions due to violations related to unlawful processing of pseudonymised data, including failing to implement adequate security measures (e.g. managing pseudonymised data with only administrator IDs and passwords), and failing to keep proper records on the processing of pseudonymised data[84].

In order to ensure compliance with the PIPA, PIPC has also conducted sectoral checks. For instance, in 2025 the PIPC conducted privacy policy evaluations for 50 companies in 7 key sectors that include big tech, online platforms and the health sector. This is part of a regular yearly exercise.

---

[80] PIPC Sanctions Meta for Violating PIPA.
[81] PIPC Announces Status Examination Results of DeepSeek Service.
[82] PIPC Sanctions AliExpress for Violating PIPA and PIPC Sanctions Temu for Unlawful Cross-Border Data Transfer and Other Violations.
[83] PIPC Sanctions SKT over Data Breach.
[84] Two public institutions sanctioned for violating personal information protection regulations.

Companies that are below the assessment thresholds set by the PIPC in advance are subject to specific improvement recommendations and are assessed again the following year[85].

The PIPC has also issued regulatory guidance. In July 2024 it published Guidelines on the Use of Publicly Available Personal Data with the aim of providing legal clarity and enhancing data protection when utilizing publicly available personal data—especially in contexts such as AI training[86]. The guidelines make clear that processing such data may be justified under the "legitimate interests" legal basis[87] and clarify that to invoke this legal basis, three conditions must be fulfilled, (i) the legitimacy of the processing purpose, (ii) the necessity of the data processing, as well as its proportionality, and (iii) a fair balance of interests between the controller and the data subject. Additionally, the guidelines suggest particular technical and organisational measures, alongside mechanisms to protect the rights of data subjects, when handling personal data that is publicly accessible.

In August 2025, the PIPC presented further guidelines for the development and use of generative AI[88]. The guidelines repeat that a controller's legitimate interests might be a suitable legal basis for processing publicly available data under the conditions of the 2024 AI guidelines. As regards the use of data collected from the data subject for the development of AI models, the guidelines explain the legal bases for processing by categorizing them into three cases: (i) where personal data are used within the original purpose of collection; (ii) where the use is reasonably related to the original purpose, in accordance with Article 15(3) of the PIPA; and (iii) where the purpose differs from the original one following , (a) pseudonymisation/anonymisation, (b) the establishment of a new legal basis in accordance with Article 18(2) of the PIPA. Furthermore, where there is a high public interest—such as in the prevention of crime—but no legal basis exists under the PIPA, or where the processing would otherwise be restricted, the regulatory sandbox system may be used, subject to the implementation of enhanced safeguards [89]. The guidelines also clarify that when the development of an AI service involves the processing of sensitive personal data, it can only be processed with separate consent or a valid legal basis.

Finally, the PIPC has carried out several awareness raising activities to ensure compliance and use of the relevant framework with stakeholders. Some of those activities concerned the EU-Korea adequacy decision. For instance, the PIPC has issued press statements and shared information about the adequacy decision and its significant impact for data flows between the EU and Korea[90]. Moreover, it has organised briefings and roundtable meetings for companies that are particularly active transferring data from the EU to Korea.

[85] Personal Information Policy Evaluation Scores Rise, Actual Service Consistency Rate Remains Low.
[86] PIPC Guideline on Processing Publicly Available Data for AI Development and Services.
[87] Article 15(1)6 of PIPA.
[88] Personal Information Processing Guide for the Development and Utilization of Generative Artificial Intelligence.
[89] The guidelines give as an example the situation where it was difficult for an autonomous driving company to improve the performance of its AI when using pseudonymised video data for AI training. A regulatory exemption was used to permit the use of original video footage without consent or pseudonymisation, under the condition of complying with enhanced security measures.
[90] PIPC Status of Recognition of Equality.

The PIPC's website is available in English and in Korean and it is updated regularly with its diverse activities. Many of the enforcement actions of the PIPC are also published in English. The Commission services note, however, that the section on international transfers could be further expanded and clarified, to ensure certainty about the specific requirements and valid systems for international transfers[91].

Since 2021 the PIPC has also deepened its cooperation with other data protection authorities in the EU. Notably, in October 2022 it signed a Declaration of cooperation with the Commission nationale de l'informatique et des libertés (CNIL), the French Data Protection Authority[92]. This framework has served as a basis for materials jointly produced by both authorities on the functioning of the data protection rules and rights for a young audience[93]. Since 2024, the PIPC and the CNIL have also held regular AI Policy bilateral meetings to exchange information on regulatory developments and emerging challenges related to artificial intelligence.

This close cooperation has also been extended to the EDPB. Since 2025, the PIPC and the EDPB have held quarterly meetings and exchanged guidelines on data protection[94].

4.1.3. Application of the Supplementary Rules in Notification 2021-5

To allow for the adoption of the adequacy decision, the Republic of Korea put in place a limited number of additional safeguards aimed at further strengthening the protection of personal information transferred from the EU to Korea, which are published in Notification 2021-5 on PIPC's website and also on the website of the National Law Information Centre in Korean [95]. The objective of these "Supplementary Rules" is to bridge certain relevant differences between the PIPA and the GDPR, and thus to guarantee that EU individuals whose personal data is transferred from the Union enjoy a level of protection essentially equivalent to that of the GDPR.

As established in Article 62 of the PIPA and Article 59 of its Enforcement Decree, the PIPC runs a Personal Information Infringement Report Centre that handles reports of violations concerning personal information rights or interests and addresses these issues through investigations. If an investigation is considered necessary, the matter is forwarded to the PIPC, which conducts investigations in line with Article 63 PIPA. Moreover, the PIPC's English-language website offers specific contact information (a hotline with phone and email) regarding the Adequacy Decision, allowing data subjects—including individuals from the EEA—to raise inquiries or concerns. In practice, since the adoption of the adequacy decision, there have been no reports of breaches of Notification No. 2021-5. Against this background, the PIPC has not conducted separate checks of compliance with the Supplementary Rules. Moreover, it has not received any complaints or been approached by EEA data subjects concerning compliance with the Supplementary Rules. Prior to the entry into force of Notification 2021-5, the PIPC published a consultation on its website about those rules. During the consultation period, no significant concerns or objections were

[91] PIPC Overseas Transfer System.
[92] Declaration of cooperation between PIPC and CNIL.
[93] « Tes données, tes droits », une affiche franco-coréenne pour sensibiliser les jeunes | CNIL.
[94] See for instance correspondence from EDBP Chair to PIPC Chairperson.
[95] See Notification No 2021-5 (Annex I) to the adequacy decision.

raised regarding the implementation of the rules. The PIPC explained that this may indicate that no major challenges have been reported by Korean controllers in applying the Notification to date.

As a result of the amendment of certain aspects of the PIPA mentioned above, some of the provisions contained in the Supplementary Rules have been now reflected in Korean law. This is a positive development which further strengthens the protection of personal data when transferred to Korea. It demonstrates that convergence between the EU and the Republic of Korea data protection frameworks has further increased since the adequacy decision was adopted.

Due to the overlap between some of the newly introduced provisions of the PIPA with some of the existing Supplementary Rules contained in Annex I to the adequacy decision (Notification 2021-5), the relevant Supplementary Rules can be revoked. As explained below, this is the case for Supplementary Rule 2, Supplementary Rule 4 and the first part of Supplementary 5. The remaining Supplementary Rules will stay in force. The PIPC will publish a new version of the Supplementary rules on its webpage.

Supplementary Rule 2 limits onward transfers of personal data pursuant to Articles 17(3) and 17(4) and Article 18 PIPA. As outlined in recital 89 of the adequacy decision, the Supplementary rule targets specific circumstances where the data could be transferred from the Republic of Korea to a third party located outside of Korea and outside of the EU/EEA if it was either reasonably related to the initial collection purpose (Article 17 PIPA) or relying on one of the exceptional circumstances mentioned in Article 18(2) PIPA. Since the third country of the receiving entity may not offer equivalent protections to those under the PIPA, Supplementary Rule 2 of Notification 2021-5 acknowledges that disadvantages may occur and that it is likely that the individual's interests may be compromised or that their rights, or those of others, may be unfairly affected. To address this situation, Supplementary Rule 2 provides that the Korean controller and third country recipient are required to establish, through a legally binding instrument (like a contract), a level of protection equivalent to the PIPA, including data subject rights.

As explained in section 4.1.1.3, Article 28-8 PIPA now establishes that no cross-border transfer of personal information shall be allowed by a personal information controller unless one of the five specific transfer tools described in that Article is applicable[96].

When personal data is provided to a third party located outside Korea, the controller must first satisfy the requirements set out in Article 17 or Article 18, as applicable, and must then also comply with the requirements of Article 28-8 PIPA concerning cross-border transfers.

As the use of a specific transfer tool is indispensable for transfers outside of Korea, even in the situations of Article 17(4) and Article 18(2) PIPA, and the conditions for international transfers have been strengthened, the Supplementary Rule 2 no longer reflects the current content of the PIPA.

[96] As explained in that section, the transfer tools allowed under Article 28-8 PIPA are essentially: 1) Separate consent of the data subject, 2) Special provisions of laws, treaties, or international agreements, 3) Processing necessary for entering into/performing a contract with the data subject, 4) Certification approved by PIPC, 5) Recognition of equivalence to the level of protection of a country/international organisation.

In addition, as has been described in section 4.1.2, the PIPC has taken an active stance in terms of international data transfers and adopted several decisions finding an infringement of the transfer rules[97]. This shows that compliance with the transfer rule remains a priority of the enforcer and that breaches are effectively investigated and sanctioned.

Supplementary Rule 4 relates to the scope of application of the special exemption to the processing of pseudonymised information. The Supplementary Rule clarified that specific provisions regarding transparency, individual rights and individual notification requirements would not apply with respect to pseudonymised information, when it is processed for the purpose of statistics, scientific research or archiving in the public interest (Article 28-7 PIPA)[98]. Moreover, the Supplementary Rule required controllers to anonymise information if the data had not been destroyed upon fulfilment of the specific purpose of processing[99].

As explained above, the changes introduced in the Republic of Korea since 2021 have brought about further convergence also in this area. In this regard, Article 28-7 PIPA has been amended to expressly clarify that certain exceptions on transparency and individual rights apply exclusively to pseudonymised data used for statistical, scientific research, or public archiving purposes[100]. Moreover, the obligation that existed to destroy personal data once the purpose had been attained or the retention period had expired, is now extended to the expiry of the processing period for pseudonymised data[101]. Therefore, unlike the situation described in recital 60 of the adequacy decision, the obligation to destroy personal data now applies when pseudonymised data is processed for statistical purposes, scientific research or archiving in the public interest.

It is also worth highlighting that PIPA contains protections prohibiting the use of the pseudonymised data to re-identify the data subject[102]. If processing pseudonymised data under such provisions generates identifiable personal data, the controller must immediately stop processing, retrieve the data and destroy it[103].

Moreover, Supplementary Rule 4 also explained the specific safeguards that exist in the PIPA to prevent the identification of individuals by third parties[104]. For instance, controllers must submit detailed documentation and send the data to be combined to a specialised institution, which generates a "combination key" to link the datasets. The specialised institution supervises the combination and release of the pseudonymised data, and any export of combined data is subject to strict conditions, including further pseudonymisation or anonymisation and approval from the institution, to prevent identification of individuals[105].

---

[97] See that section for the summary and press release of the decisions in the cases of DeepSeek, Temu or AliExpress.
[98] Recital 82 of the adequacy decision.
[99] Recital 60 of the adequacy decision.
[100] The Article now reads: Articles 20, 20-2,27, 34 (1), 35, 352, 36, and 37 shall not apply to pseudonymised information processed under Article 28-2 or 28-3 PIPA.
[101] The obligation in Article 21 PIPA applies now to pseudonymised data as it is no longer mentioned among the derogations in Article 28-7 PIPA.
[102] Article 28-5 PIPA.
[103] Article 28-5 (2) PIPA.
[104] Recitals 46 to 48 of the adequacy decision.
[105] Article 28-3 PIPA.

As explained in section 4.1.1.1, the rules on pseudonymisation have been enforced by the PIPC that has adopted specific decisions and sanctions. Moreover, those rules have also been interpreted by the Supreme Court, that has found that when a reasonable risk of re-identification exists, data must still be considered personal data, and the full protection of the PIPA continues to apply[106]. This indicates that compliance with such rules remains an enforcement priority. Accordingly, as further clarity has been ensured in the Republic of Korea concerning the conditions for the use of this derogation for statistical, scientific research, or public archiving purposes and there is now a general obligation to destroy personal data once the specific purpose has been achieved, the Supplementary Rule overlaps with the provisions of the PIPA.

Supplementary Rule 5 refers to the possibility by the PIPC of adopting corrective measures. As explained in recital 120 of the adequacy decision concerning the version of the PIPA in force at the time of its adoption, under Article 61(2) PIPA, the PIPC could provide advice to controllers on how to improve the level of personal data protection of specific processing activities. Controllers had to make good faith efforts to implement such advice and were required to inform the PIPC of the outcome. Moreover, when there were reasonable grounds to believe that a violation of PIPA had occurred and failure to take action was likely to cause damage difficult to remedy, the PIPC had the power to impose corrective measures (Article 64(1) PIPA). The first part of Supplementary Rule 5 concerned Article 64(1) PIPA and clarified, with binding effect, that those conditions in Article 64(1) PIPA were fulfilled with respect to the violation of any PIPA provision that protects the privacy rights of individuals with respect to personal information[107].

As it has been explained in section 4.1.2, under the new provisions of Article 64(1) PIPA and Article 64(2) PIPA, the reference to such reasonable grounds has been removed[108]. Accordingly, the clarification introduced by the Supplementary Rule concerning Article 64(1) PIPA and Article 64(2) PIPA has become redundant.

Supplementary Rule 5 also introduced specific clarifications regarding Article 64(4) PIPA and the enforcement vis-à-vis certain public authorities[109]. That provision is now included in Article 64(3) PIPA, after some changes as part of the 2023 PIPA amendment. Nevertheless, there has been no substantial change to the content of that provision and the part of Supplementary Rule 5 concerning Article 64(4) PIPA continues to remain in force.

---

[106] See section 4.1.1.1 above.

[107] That first part reads: (i) First, court precedents 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.

[108] The article now reads instead: The Protection Commission may order a person who violates this Act (excluding central administrative agencies, local governments, the National Assembly, the Court, the Constitutional Court, and the National Election Commission) to take the following measures: 1. To suspend personal information breach; 2. To temporarily suspend personal information processing; 3. Other measures necessary to protect personal information and to prevent personal information infringement.

[109] See for further explanations in this regard recital 121 of the adequacy decision.

4.2. Aspects relating to access and use of personal data by the authorities in the Republic of Korea

4.2.1. Legislative and policy developments in the Republic of Korea

The adequacy decision contains an assessment by the Commission of the safeguards and limitations, including oversight and mechanisms for individual redress, that are provided by Korean law, concerning the collection of and subsequent use of personal data transferred from the EU by Korean public authorities for purposes of public interest, in particular in relation to criminal enforcement and national security. The mechanisms for redress also included a specific possibility for EU individuals to submit a complaint to the PIPC through their data protection authority[110]. Following its analysis and also taking into consideration the specific representations, assurances and commitments signed at the highest ministerial and agency level that are contained in Annex II to the adequacy decision, the Commission found that any government access in the Republic of Korea would be restricted to what is strictly necessary and that there are effective safeguards in place to protect against interferences[111].

Since the adoption of the adequacy decision, there have been amendments to several laws that were assessed for the adequacy finding concerning the Republic of Korea. A notable change concerns the Telecommunications Business Act. In a judgment delivered in 2022, the Constitutional Court found that the absence of post-notification procedures concerning the access to telecommunications subscriber data constituted a breach of the constitutional right to informational self-determination [112] . Accordingly, Article 83-2 of the Telecommunications Business Act was amended. Under the new provision, law enforcement and other authorised agencies that have obtained subscriber information from telecommunications providers are now obliged to notify the individual concerned within 30 days, unless special circumstances are applicable. Furthermore, the notification must contain essential details of the data access request and its purpose.

During the review meeting, the PIPC expanded on the concept of such special circumstances that would prevent the notification. Article 83-2(4) of the Telecommunications Business Act provides for exceptions to the post-notification requirement for access to telecommunications subscriber data. Specifically, authorities are not required to notify the data subject if the request for access involves either foreign institutions, organisations, or individuals suspected of engaging in anti-state activities or acting in hostility toward the Republic of Korea, as well as Korean nationals affiliated with such entities; or groups located in areas within the Korean Peninsula that are beyond the de facto jurisdiction of the Republic of Korea, or organisations abroad that are subordinate to such groups, including Korean nationals affiliated with them.

Therefore, as clarified by the Korean authorities, the provision is intended to address exceptional national security risks and the exceptions to the general notification requirement are aimed at

[110] See Notification No 2021-5 (Section 6, Annex I). See also recital 205 of the adequacy decision.
[111] See also Section 3 to the adequacy decision.
[112] Judgment of the Constitutional Court of Korea in Case 2016Hun-Ma388 of 21 July 2022.

ensuring that such obligations do not compromise ongoing investigations involving serious threats to the state.

Moreover, the Communications Privacy Protection Act (CPPA) has been amended on three occasions since the adoption of the adequacy decision[113]. A December 2022 amendment strengthened oversight over emergency communication interception measures. As described in recital 189 of the adequacy decision with respect to access by Korean authorities to communication information for national security purposes, warrantless collection may only take place if there is an act of conspiracy that threatens national security and if there is an emergency that makes it impossible to go through the standard procedures. Following the 2022 amendment, the oversight over such emergency communication interception measures has been strengthened. Pursuant to the new provisions in Article 8 of the Act, even if such emergency interception measures are terminated within a short period of time, ex-post court approval is now required[114]. Moreover, if the court does not grant its approval within 36 hours of initiating the emergency interception measure, any data collected through such action must be destroyed and such destruction reported to the court[115].

A further amendment to the CPPA in 2024 strengthened the reporting obligations for telecommunication business entities, who pursuant to Article 13(7) CPPA are required to report every six months to the Minister of Science and Information and Communication Technology (ICT) on the communication data they provide to authorities and retain related records for seven years. A new Article 15-3 CPPA provides the Minister with the power to adopt corrective orders in case the obligations of Article 13(7) CPPA are not complied with. Moreover, if such order is not followed, the Minister now has the power to impose a fine[116].

In terms of other regulatory developments, the Regulation on Cooperation between Prosecutors and Judicial Police Officers and General Investigation Rules was amended in October 2023[117], and data minimization and procedural safeguards in the context of search and seizure operations by criminal law enforcement authorities were strengthened. Moreover, the procedures for providing a copy of the warrant during a search, seizure, or inspection carried out under warrant authority have been made more explicit[118]. There is now an obligation to adopt measures, when presenting or delivering a warrant or its copy, to prevent undue exposure of personal information belonging to victims or other individuals connected to the case.

---

[113] https://www.law.go.kr/LSW/eng/engLsSc.do?menuId=2&section=lawNm&query=%ED%86%B5%EC%8B%A0%EB%B9%84%EB%B0%80&x=0&y=0#liBgcolor1: Act No. 19103, Dec. 27, 2022, Act No. 20072, Jan. 23, 2024 and Act No. 20735, Jan. 31, 2025. The 2025 amendment concerns licences for distributing wiretapping equipment.

[114] Article 8 (2) CPPA. Such emergency communication-restricting measures may only be used in very limited circumstances, namely if there is an act of conspiracy that threatens the national security, in the case of the planning or execution of any serious or organised crime, or if any similar event is imminent that may directly cause death or serious injury, and if in addition there is an emergency that makes it impracticable to follow the normal procedures.

[115] Article 8 (5) CCPA and Article 8 (6) CPPA.

[116] Article 15-4 CPPA.

[117] https://www.law.go.kr/lsInfoP.do?lsId=013871&ancYnChk=0#0000.

[118] Article 38 of that Regulation.

The PIPC has also strengthened its oversight of public authorities and bodies by promoting compliance with certain key principles of data protection. In December 2024, the PIPC developed, in cooperation with other relevant institutions, the Public Sector Guidelines on Personal Data Protection[119]. These guidelines aim to ensure that public authorities strictly adhere to data protection principles when handling personal data. and focus in particular on how important principles such as data minimization, purpose limitation, integrity and confidentiality, and storage limitation can be implemented in practice[120].

4.2.2. Oversight and Enforcement Activities of the PIPC and other bodies

As explained in the adequacy decision, different bodies in the Republic of Korea have oversight and enforcement powers with respect to criminal law enforcement and national security authorities. Since the adoption of the adequacy decision, the PIPC and the National Human Rights Commission of Korea (NHRCK) have been particularly active in this area.

For example, as explained by the PIPC as part of the review, the PIPC in September 2024 advised the National Intelligence Service (NIS) on the lawfulness of personal data processing for national security purposes under the PIPA and related legislation. The PIPC's advice was based on a comprehensive review of the applicable legal provisions and included an assessment of the legality of the specific data processing activities, as well as guidance on appropriate security measures that must be implemented to safeguard personal information.

Following specific requests by other public authorities, the PIPC also adopted different types of public resolutions establishing how data should be handled in specific circumstances. This concerned for instance the provision of personal data by the Ministry of Justice to the National Police Agency for counter-terrorism purposes. According to the Resolution adopted on 13 April 2022, in situations where the National Police Agency is unable to confirm the identities of individuals suspected of terrorism or related activities, it is permitted to share photographs of these suspects with the Ministry of Justice as a supplementary, exceptional measure[121]. The Ministry of Justice may then disclose the individual's name, date of birth, gender, nationality, passport number, and ID registration number, provided that the photograph matches with a high likelihood of correct identification.

A similar resolution concerned the fight against telecommunications fraud. On 12 March 2025, the PIPC authorised the National Police Agency to collect the sender's phone number when a recipient reports a suspected fraud-related text message via the Simple Reporting System to prevent telecommunications and financial fraud. Additionally, under the provisions of the PIPA, that agency may acquire necessary details from mobile carriers to block web accounts responsible for

[119] Personal Information Protection Guidelines (Public Institutions Edition). The other institutions involved included the Office for Government Policy Coordination, Board of Audit and Inspection (BAI), Ministry of Justice, and Korean National Police Agency.

[120] See section 3.1 of the guidelines, focused on Matters related to investigative work, the Criminal Procedure Act, Criminal Procedure Electronic Act, etc.

[121] See Resolution of Personal Information Protection Committee of 13 April 2022 on request for provision of personal information held by the Ministry of Justice for the conduct of counterterrorism counterintelligence information activities by the National Police Agency.

sending these fraudulent messages. These measures aim to mitigate the damage caused by such scams. Overall, the agency seeks to enhance prevention and protection against telecommunication and financial fraud[122].

The NHRCK on 24 March 2023 recommended the head of a District Prosecutors' Office to issue a warning to an investigated person and conduct staff training to prevent the wrongful disclosure of suspects' criminal records during investigations[123]. The NHRCK found that a criminal record contains sensitive personal information, and its exposure can severely impact an individual's dignity, warranting careful management to avoid leaks during investigative proceedings. Similarly, on 6 August 2025, it recommended disciplinary action against a police officer for misuse of personal data obtained in the course of handling a criminal case[124].

The NHRCK has also been active in its advisory role. For instance, in 2022 it advised on the amendment to the Telecommunications Business Act to address the unjustified collection of communication data by investigative agencies[125]. Similarly, in 2025 it issued a recommendation to change Court regulations on personal data clarifying that sending penalty decisions to case parties without anonymizing personal information could infringe their right to data protection[126].

[122] See resolution of Personal Information Protection Committee of 12 March 2025 on request for the Collection and Provision of Personal Information for the Prevention of Electrofinancial, Telecommunications Fraud by the National Police Agency.
[123] Case No. 22jinjeong0220300 – See a refence in English in: https://www.humanrights.go.kr/base/board/read?boardManagementNo=18&boardNo=7611096&searchCategory=&page=1&searchType=&searchWord=&menuLevel=3&menuNo=114.
[124] See in English: https://www.humanrights.go.kr/eng/board/read?boardManagementNo=7003&boardNo=7611564&searchCategory=&page=1&searchType=total&searchWord=personal%20data&menuLevel=2&menuNo=114.
[125] See recommendations included in its Annual Report 2022 - https://www.humanrights.go.kr/base/board/read?boardManagementNo=18&boardNo=7609407&searchCategory=&page=1&searchType=&searchWord=&menuLevel=3&menuNo=114.
[126] https://www.humanrights.go.kr/eng/board/read?boardManagementNo=7003&boardNo=7611519&searchCategory=&page=1&searchType=total&searchWord=personal%20data&menuLevel=2&menuNo=114.