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

Version 1.0

Adopted on 24 September 2021

CONTENTS

The European Data Protection Board

Having regard to Article 70(1)(s) of the Regulation 2016/679/EU 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 of the free movement of such data, and repealing Directive 95/46/EC ("**GDPR**"),

Having regard to the European Economic Area ("**EEA**") Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[1],

Having regard to Article 12 and Article 22 of its Rules of Procedure,

HAS ADOPTED THE FOLLOWING OPINION:

1. EXECUTIVE SUMMARY

1. The European Commission launched the formal process towards the adoption of its draft implementing decision ("**draft decision**") on the adequate protection of personal data in the Republic of Korea under the Personal Information Protection Act pursuant to the GDPR on 16 June 2021[2].

2. On the same date, the European Commission asked for the opinion of the European Data Protection Board ("**EDPB**")[3]. The EDPB's assessment of the adequacy of the level of protection afforded in the Republic of Korea has been made on the basis of the examination of the draft decision itself as well as on the basis of an analysis of the documentation made available[4] by the European Commission.

3. The EDPB focused on the assessment of both, the general GDPR aspects of the draft decision and the access by public authorities to personal data transferred from the EEA for the purposes of law enforcement and national security, including the legal remedies available to individuals in the EEA. The EDPB also assessed whether the safeguards provided under the Korean legal framework are in place and effective.

4. The EDPB has used as main reference for this work its GDPR Adequacy Referential[5] ("**GDPR Adequacy Referential**") adopted in February 2018 and the EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures[6].

1.1. Areas of convergence

5. The EDPB's key objective is to give an opinion to the European Commission on the adequacy of the level of protection afforded to individuals whose personal data is transferred to the Republic of Korea.

[1] References to "**Member States**" made throughout this opinion should be understood as references to "EEA Member States".
[2] See press release https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2964.
[3] Ibid.
[4] The EDPB based its analysis on official translations prepared by the Korean government.
[5] WP254, GDPR Adequacy Referential, 6 February 2018, (endorsed by the EDPB, see https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines).
[6] See EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, adopted on 10 November 2020, https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_en.

It is important to recognise that the EDPB does not expect the Korean data protection framework to replicate European data protection law.

6. However, the EDPB recalls that, to be considered as providing an adequate level of protection, Article 45 GDPR and the case-law of the Court of Justice of the European Union (hereinafter "**CJEU**") require the third country's legislation to be aligned with the essence of the fundamental principles enshrined in the GDPR. In this context, the Korean data protection framework presents numerous similarities to the European data protection framework, having one main piece of legislation covering both, the public and the private sector, and which is completed by sector-specific legislative acts.

7. With regards to the content, the EDPB notes key areas of alignment between the GDPR framework and the Korean data protection framework with regard to certain core provisions such as, for example, concepts (e.g., "personal information", "processing", "data subject"); grounds for lawful and fair processing for legitimate purposes; purpose limitation; data quality and proportionality; data retention, security and confidentiality; transparency; and special categories of data.

8. In addition to the above, the EDPB welcomes the efforts made by the European Commission and the Korean authorities to ensure that the Republic of Korea provides an adequate level of protection to that of the GDPR through the adoption of Notifications by the Korean supervisory authority (applicable not only to personal data transferred from the EEA to Korea) with the aim to fill in the gaps between the GDPR and the Korean data protection framework. In this context, the EDPB wishes to highlight the relevance of these Notifications for the assessment of the adequacy of the Republic of Korea noting, for example, that they provide relevant clarifications on some important safeguards, inter alia in relation to the scope of application of the exemptions from the PIPA for the processing of pseudonymised personal information for scientific, research and statistical purposes, onward transfers and the rules applicable in the context of access to data by public authorities.

1.2. Challenges

9. While the EDPB has identified many aspects of the Korean data protection framework to be essentially equivalent to the European data protection framework, it has also concluded that there are certain aspects that may require a closer look and clarification. Specifically, the EDPB considers that the following items should be further assessed to ensure that the essentially equivalent level of protection is met, and that they should be closely monitored by the European Commission.

1.2.1. General

10. The EDPB takes note that the Notification No 2021-1 *has the status of an administrative rule with legally binding force on the personal information controller in the sense that any violation of th[e] Notification may be regarded as a violation of the relevant provisions of PIPA*[7]. However, considering that the Notification does not include additional rules per se but rather clarifications on how the statutory text of PIPA should be understood to apply and in light of its overall importance particularly with respect to the pseudonymisation provisions under PIPA which the EDPB understands are the object of ongoing judicial cases, the EDPB invites the European Commission to provide further information on the binding nature, the enforceability and validity of Notification No 2021-1 and would recommend an attentive monitoring of its respect in practice, in particular with regard to its application not only by the Korean supervisory authority but also by courts, especially where the equivalent level of protection afforded by the Korean legal framework is based on the clarifications provided for therein.

[7] See Section I of Annex I of the draft decision.

1.2.2. General data protection aspects

11. In relation to the scope of application of the adequacy decision, the EDPB notes that it will cover transfers from the EEA legal framework to both, public and private "personal information controllers" falling under the scope of the PIPA. The EDPB understands that entities acting as processors within the meaning of the GDPR are included in this term, however, in order to avoid misunderstandings, it invites the European Commission to make it clearer that the adequacy decision will also cover transfers to "processors" in Korea.

12. An important aspect that the EDPB would like to call the attention to relates to the concept of pseudonymised information in the Korean data protection framework. Under Korean law, exemptions from a number of relevant provisions, including those on individual data subject rights and data retention, apply to the processing of pseudonymised personal information. According to the European Commission, this is only the case where pseudonymised personal information is processed for the purposes of statistics, scientific research or archiving in the public interest. However, this assertion is mainly supported by Notification No 2021-1 which makes the already mentioned need for additional information about and the monitoring of the binding nature, enforceability and validity of this Notification highly relevant in this context. In addition, the EDPB invites the European Commission to further assess the impact of pseudonymisation under Korean law and, most importantly, how it may affect the fundamental rights and freedoms of data subjects whose personal data is transferred to the Republic of Korea under the adequacy decision. In particular, the EDPB calls on the European Commission to assess further the derogations contained in Article 28(7) PIPA and Article 40(3) CIA and to attentively monitor their application and relevant case law in order to ensure that the data subject rights are not be unduly restricted when personal data transferred under the adequacy decision is processed for these purposes.

13. Further, the EDPB notes that under Korean law a right to withdraw consent exists only in specific circumstances and therefore invites the European Commission to further assess the impact of a lack of a general right to withdraw consent and to provide further assurances so as to ensure than an essential level of data protection is guaranteed at all times also, where necessary, by clarifying the role of the right to suspension under PIPA in the absence of a general right to withdraw consent.

14. With regard to onward transfers, the EDPB acknowledges that informed consent of the data subject will be generally used as a basis for data transfers from a Korean-based personal information controller to a third country-based recipient and that Notification No 2021-1 envisages that individuals must be informed about the third country to which their data will be provided. However, the EDPB invites the European Commission to ensure that the information to be provided to the data subject also includes information on the possible risks of transfers arising from the absence of adequate protection in the third country as well as the absence of appropriate safeguards. Furthermore, the EDPB would welcome reassurances in the adequacy decision that personal data will not be transferred from Korean personal information controllers to a third country in any situation in which under the GDPR valid consent could not be provided, e.g. because of an imbalance of power.

15. With regard to the appointment of the members of the Korean supervisory authority, although the formal procedure would be in line with GDPR and therefore meet the test of equivalence with the EEA legal framework, the EDPB would welcome the European Commission to monitor any developments that might affect the independence of the members of the South Korean supervisory authority.

16. Regarding the budget, again based on the information provided by the European Commission, no reference is made to the specificities of the staff assigned to the PIPC nor to the financial resources made available to it. The EDPB would therefore welcome additional information in the draft decision on these two relevant topics.

1.2.3. On the access by public authorities to data transferred to the Republic of Korea

17. The EDPB has also analysed the Korean legal framework with respect to government access for law enforcement and national security purposes to personal data transferred from the EEA to Korea. While acknowledging the representations and assurances provided by the Korean government, as outlined in Annex II of the draft decision, the EDPB has identified a number of aspects that require clarification or raise concerns.

18. The EDPB notes that PIPA's provisions apply without limitation in the area of law enforcement. The EDPB also notes that data processing in the area of national security is subject to a more limited set of provisions enshrined in PIPA.

19. With regard to the voluntary disclosure of personal information by telecommunication providers to national security authorities the EDPB is concerned that the relationship of Section 3 of Annex I of the draft decision which specifies that providers in principle have to notify the concerned individual when they voluntarily comply with a request, and Article 58(1) lit. 2 PIPA, i.e., the partial exemption for national security purposes, is unclear. This could render information requirements ineffective, making it considerably more difficult for data subjects to assert their data protection rights especially with regard to judicial redress.

20. While the draft decision does not explicitly say so, the EDPB understands from the explanations provided by the European Commission that the Korean legal framework does not allow for the interception of telecommunication data in bulk. Therefore, the recent case law of the European Court of Human Rights ("**ECtHR**") on bulk interception regimes would not be directly relevant for the assessment of the level of data protection in Korea.

21. The draft decision does not contain any information on the legal framework for onward transfers in the area of national security. While the EDPB understood that, in the view of the European Commission, onward transfers for national security purposes are sufficiently regulated by the general safeguards and principles following from the constitutional framework and PIPA, the EDPB is concerned as to whether this can be considered to meet the requirements of preciseness and clarity of the law and enshrines effective and enforceable safeguards. The safeguards the European Commission refers to are of a very general nature and do not address, in a legal basis, the specific circumstances and conditions under which onward transfers for national security purposes may take place. In this context, the EDPB also notes that the European Commission did not consider the existence of international agreements concluded between the Republic of Korea and third countries or international organisations that may provide for specific provisions for the international transfer of personal data by law enforcement and/or intelligence services to third countries. The EDPB considers that the conclusion of bilateral or multilateral agreements with third countries for the purposes of law enforcement or intelligence cooperation is likely to affect the Korean data protection legal framework as assessed.

22. The EDPB notes that the oversight of criminal law enforcement as well as national security authorities is ensured by a combination of different internal and external bodies, in particular the PIPC, which is endowed with sufficient executive powers.

23. Effective remedies and redress require that data subjects are able to turn to a competent body that meets the requirements of Article 47 of the Charter of Fundamental rights of the European Union ("**the Charter**"), i.e., which is competent to determine that a data processing is taking place, to verify the lawfulness of the processing, and which has enforceable remedial powers in the event the data processing is unlawful. Against this background, the EDPB asks the European Commission to clarify whether a complaint with the PIPC or any action before a court is subject to substantive and/or procedural requirements, such as a burden of proof, and whether individuals in the EEA would be able to meet such precondition.

1.3. Conclusion

24. The EDPB considers that this adequacy decision is of paramount importance also taking into account that – with the exceptions highlighted in the opinion – it will cover transfers both, in the public and private sector.

25. The EDPB welcomes the efforts made by the European Commission and the Korean authorities to align the Korean legal framework with the European one. The improvements intended to be brought in by Notification No 2021-1 to bridge some of the differences between the two frameworks are very important and well received. However, the EDPB notices that a number of concerns, including with regard to Notification No 2021-1, coupled with the need for further clarifications on other issues, remain, and it recommends the European Commission to address the concerns and requests for clarification raised by the EDPB and provide further information and explanations regarding the issues raised in this opinion.

2. INTRODUCTION

2.1. Korean data protection framework

26. The main piece of legislation governing data protection in the Republic of Korea is the Personal Information Protection Act (Act No. 10465 of 29 March 2011, last amended by Act No. 16930 of 4 February 2020, "**PIPA**"). 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 is legally binding and enforceable.

27. In addition to PIPA, the Korean data protection framework includes regulatory "Notifications" issued by the Korean supervisory authority, the Personal Information Protection Commission ("**PIPC**"), providing further rules on the interpretation and application of PIPA. Recently, the PIPC adopted Notification No 2021-1 of 21 January 2021 (which amended the previous Notification No 2020-10 of 1 September 2020, hereafter "**Notification No 2021-1**") on the interpretation, application and enforcement of certain provisions of PIPA. More specifically, this Notification resulted from adequacy discussions held between Korean authorities and the European Commission. It contains clarifications on the application of specific provisions of PIPA, including concerning the processing of personal data transferred to Korea based on the envisaged adequacy decision[8] and it *has the status of an administrative rule with legally binding force on the personal information controller in the sense that any violation of th[e] Notification may be regarded as a violation of the relevant provisions of PIPA*[9]. In this context, the EDPB would like to note that, despite being referred to as "Supplementary Rules" in the draft decision, the Notification does not include additional rules *per se* but rather explanations aimed at clarifying how the statutory text of PIPA should be understood to apply, in particular with respect to data transferred from the EEA. Against this background, the EDPB would recommend an attentive monitoring of the respect of Notification No 2021-1 in practice, in particular with regard to their application not only by the PIPC but also by courts, especially where the equivalent level of protection afforded by the Korean legal framework is based on the clarifications provided for in the Notification No 2021-1.

28. Other relevant data protection laws in the Korean legislative framework lay down rules to the processing of personal data in specific industry sectors such as:

- The Act on the Use and Protection of Credit Information ("**CIA**"), including its Enforcement Decree ("**CIA Enforcement Decree**"), which lay down specific rules applicable to

[8] See Section I of Annex I of the draft decision.
[9] Ibid.

commercial operators and specialised entities (such as credit rating agencies, financial institutions) when they process personal credit information necessary to determine the creditworthiness of parties to financial or commercial transactions;

- The Act on the Promotion of Information and Communications Network Utilisation and Data Protection ("**Network Act**"); and
- The Communications Privacy Protection Act ("**CPPA**")

29. In the area of government access, apart from the relevant provisions contained in the PIPA and the CPPA, the EDPB has considered some other pieces of legislation, i.e., the Criminal Procedure Act ("**CPA**"), the Telecommunications Business Act ("**TBA**"), the Act on Reporting and Using Specified Financial Transaction Information ("**ARUSFTI**") and the National Intelligence Service Act ("**NISA**").

2.2. Scope of the EDPB's assessment

30. The draft decision of the European Commission is the result of an assessment of the Korean data protection framework, followed by discussions with the Korean government. In accordance with Article 70(1)(s) GDPR, the EDPB is expected to provide an independent opinion on the European Commission's findings, identify insufficiencies in the adequacy framework, if any, and endeavour to make proposals to address these.

31. In order to avoid repetition and with the aim to helping in the assessment of the Korean legal framework, the EDPB has chosen to focus on some specific points presented in the draft decision and provide its analysis and opinion on them, refraining from reproducing most of the factual findings and assessments where the EDPB has no indication to assume that the law of the Republic of Korea would not be essentially equivalent to the law in the EEA. In addition, in line with the jurisprudence of the CJEU, a very important part of the analysis covers the legal regime of national security access to the personal data transferred to the Republic of Korea, and the practice of its national security apparatus.

32. In its assessment, the EDPB took into account the applicable European data protection framework, including Articles 7, 8 and 47 of the Charter, respectively protecting the right to private and family life, the right to protection of personal data and the right to an effective remedy and fair trial, and Article 8 ECHR protecting the right to private and family life. In addition to the above, the EDPB considered the requirements of the GDPR as well as the relevant case law.

33. The objective of this exercise is to provide the European Commission with an opinion on the assessment of the adequacy of the level of protection in the Republic of Korea. The concept of "adequate level of protection" which already existed under Directive 95/46, has been further developed by the CJEU. It is important to recall the standard set by the CJEU in Schrems I, namely that – while the "level of protection" in the third country must be "essentially equivalent" to that guaranteed in the EU – "*the means to which that third country has recourse, in this connection, for the purpose of such a level of protection may differ from those employed within the EU*"[10]. Therefore, the objective is not to mirror point by point the European legislation, but to establish the essential and core requirements of the legislation under examination. Adequacy can be achieved through a combination of rights for the data subjects and obligations on those who process personal data, or who exercise control over such processing and supervision by independent bodies. However, data protection rules are only effective if they are enforceable and followed in practice. It is therefore necessary to consider not only the content of the rules applicable to personal data transferred to a third country or an international organisation, but also the system in place to ensure the effectiveness

[10] C-362/14, *Maximilian Schrems v Data Protection Commissioner*, 6 October 2015, ECLI:EU:C:2015:650, paras. 73-74.

of such rules. Efficient enforcement mechanisms are of paramount importance to the effectiveness of data protection rules[11].

2.3. General comments and concerns

2.3.1. International commitments entered into by the Republic of Korea

34. According to Article 45(2)(c) GDPR and the GDPR Adequacy Referential[12], when assessing the adequacy of the level of protection of a third country, the European Commission shall take into account, among others, the international commitments the third country has entered into, or other obligations arising from the third country's participation in multilateral or regional systems, in particular in relation to the protection of personal data, as well as the implementation of such obligations.

35. 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). Furthermore, Korea, as an OECD member, adheres to the OECD Privacy Framework, in particular the Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data.

36. The EDPB also takes note of the participation of Korea as Observer State in the work of the Consultative Committee of the Council of Europe Convention 108(+), although it has not yet decided whether to accede.

2.3.2 Scope of the adequacy decision

37. According to Recital 5 of the draft decision, the European 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 to personal information controllers (e.g. natural or legal persons, organisations, public institutions) falling within the scope of application of PIPA, with the exception of processing of personal data for missionary activities by religious organisations and for the nomination of candidates by political parties[13], or the processing of personal credit information pursuant to the CIA by controllers that are subject to oversight by the Financial Services Commission.

38. The EDPB notes that the adequacy decision will cover transfers from the EEA legal framework to both, public and private "personal information controllers" falling under the scope of the PIPA. The EDPB understands that entities acting as processors within the meaning of the GDPR are also covered by the term "personal information controller" considering that the PIPA will apply equally to them and that specific obligations apply when a personal information controller (the "outsourcer") engages a third party for the processing of personal information (the "outsourcee"), however, in order to avoid misunderstandings, the EDPB invites the European Commission to make it clearer that the adequacy decision will also cover transfers to "processors" in Korea and that the level of protection of personal data transferred from the EEA will not be undermined also in these cases.

39. Besides, taking into account that the adequacy decision also covers personal data transfers between public bodies, the EDPB understands that this will also cover transfers between data protection supervisory authorities and, for the sake of clarity, invites the European Commission to specifically address this issue.

[11] WP254, p.2.
[12] WP254, p.2.
[13] For more context see below under section 3.1.2 of this opinion.

40. Furthermore, with regards to the entities excluded from the scope of application of the adequacy decision, the EDPB would like to emphasise that the adequacy decision could benefit from a clearer identification of the "commercial organisations" that are subject to the oversight of the PIPC (Article 45(3) CIA) so that EEA-based controllers and processors may easily assess whether the importer falls also under the scope of application of the adequacy decision before transferring data to entities falling under the scope of application of the CIA or, at least, be alerted of the need to assess this aspect.

41. With respect to the scope of the adequacy decision, the EDPB understood from the additional explanations of the European Commission that the Korea Financial Intelligence Unit ("**KOFIU**"), which is established under the Financial Services Commission and oversees the prevention of money laundering and terrorist financing pursuant to the ARUSFTI[14], is also excluded from the scope, as it has only jurisdiction over financial institutions which are themselves not covered by the draft decision. However, Article 1(2)(c) of the draft decision excludes from its scope only those personal information controllers that are subject to oversight by the Financial Services Commission and process personal credit information under the CIA. Against this background, the EDPB asks the European Commission to clarify whether the KOFIU and the data processing activities undertaken by KOFIU itself fall under the draft decision.

3. GENERAL DATA PROTECTION ASPECTS

3.1. Content principles

42. Chapter 3 of the GDPR Adequacy Referential is dedicated to the "Content Principles". A third country's system must contain them in order to regard the level of protection provided as essentially equivalent to the one guaranteed by EU legislation.

43. Although the right to the protection of personal data is not expressly enshrined in the Korean Constitution per se, it is 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 and the Constitutional Court, as referenced in the European Commission's draft decision[15]. The EDPB takes notes of this recognition since it derives from it that data protection as a basic right, according to Article 37 of the Korean Constitution, "*may only be restricted by law and when necessary for national security, or the maintenance of law and order or for public welfare*" and that "*even when such restrictions are imposed, they may not affect the essence of the freedom or right*".

44. According to the European Commission[16], the Constitutional Court has ruled that also foreign nationals are the subject of basic rights. As per the official representations from the Korean government[17], although case law has so far not specifically dealt with the right to privacy by non-Korean nationals, it is widely accepted among scholars that Articles 12-22 of the Constitution set out "rights of human beings". Further, the Republic of Korea has enacted a series of laws in the area of data protection that provide safeguards for all individuals, irrespective of their nationality, such as the PIPA. In this regard, the EDPB takes note that Article 6(2) of the Constitution provides that the status of foreign nationals is guaranteed as prescribed by international law and treaties and of the case law mentioned in the draft decision according to which a "foreigner" can be the bearer of "basic rights". Considering the relevance of the recognition of the right to data protection to "foreign nationals", the EDPB calls the attention of the European Commission on the need to keep monitoring the case law

[14] See Annex II, section 2.2.3.1.
[15] See Recital 8 of the draft decision and the relevant case law referred to in footnote 10 of the draft decision of which only English summaries are available.
[16] See Recital 9 of the draft decision.
[17] Section 1.1. of Annex II of the draft decision.

relating to data protection as a basic right recognised not only to Korean citizens but to all data subjects so as to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data are transferred to Korea under the adequacy decision.

3.1.1. Concepts

45. Based on the GDPR Adequacy Referential, basic data protection concepts and/or principles should exist in the third country's legal framework. Although these do not have to mirror the GDPR terminology, they should reflect and be consistent with the concepts enshrined in the European data protection law. For example, the GDPR includes the following important concepts: "personal data", "processing of personal data", "data controller", "data processor", "recipient" and "sensitive data"[18].

46. The PIPA includes a number of definitions such as, among others, those of "personal information", "processing" and "data subject", which closely resemble the corresponding terms under the GDPR.

3.1.1.1. Concept of pseudonymised data

47. Among the definitions provided in the PIPA, Article 2(1) PIPA defines, in particular, personal information as any of the following information relating to a living individual: (a) information that identifies a particular individual by his or her full name, resident registration number, image, etc. and (b) information which, even if it by itself does not identify a particular individual, may easily be combined with other information to identify a particular individual. In the latter cases, whether or not there is ease of combination shall be determined by reasonably considering the time, cost, technology, etc. used to identify the individual such as the likelihood that the other information can be procured.

48. In addition, according to Article 2(1) lit. (c) PIPA, also "pseudonymised information" is considered personal information. Pseudonymised information is defined as information under items (a) or (b) above that is pseudonymised in accordance with subparagraph 1-2 and thereby becomes incapable of identifying a particular individual without the use or combination of information for restoration to the original state. Information that is fully anonymised is excluded from the scope of application of the PIPA. According to Article 58(2) PIPA, the act does not apply to information that no longer identifies a certain individual when combined with other information, reasonably considering time, cost, technology, etc.

49. The European Commission states in Recital 17 of its draft decision that this corresponds with the material scope of application of the GDPR and its notions of "personal data", "pseudonymisation" and "anonymised information".

50. However, according to Article 28(7) PIPA, Articles 20, 21, 27, 34(1), 35 through 37, 39(3), 39(4), 39(6) through 39(8) do not apply to pseudonymised personal information.

51. In its draft decision, the European Commission states that Article 28(7) PIPA is only applicable to pseudonymised personal information when it is processed for the purposes of statistics, scientific research or archiving in the public interest[19]. However, this does not follow directly from the letter of the law but from the explanations provided in Notification No 2021-1[20]. While the EDPB acknowledges that an argument can be made based on the structure and rationale of PIPA that Article 28(2) PIPA should be understood and logically interpreted as also applying to Article 28(7) PIPA, in light of the importance of Notification No 2021-1 in the European Commission's assessment of the adequacy of the level of protection of personal data in the Republic of Korea and to avoid any doubt, the EDPB

[18] WP254, p. 4.
[19] See *inter alia* Recital 82 of the draft decision.
[20] Section 4 of Annex I to the draft decision.

invites the European Commission to provide further information on the binding nature, enforceability and validity of Notification No 2021-1 and to monitor its application in this specific context.

52. In this context, the EDPB would like to recall that under the GDPR pseudonymisation is understood as a recommended security measure. In other words, under the GDPR pseudonymised data remains personal data to which the GDPR fully applies. Based on the foregoing, the EDPB has concerns that the GDPR's level of protection of pseudonymised personal data could be undermined when personal data are transferred to Korea. The EDPB therefore invites the European Commission to further assess the impact of pseudonymisation under the PIPA and, most importantly, how it may affect the fundamental rights and freedoms of data subjects whose personal data would be transferred to the Republic of Korea on the basis of the adequacy decision. Hence, the EDPB calls upon the European Commission to provide assurances that the level of protection of personal data from data subjects in the EEA will not be lowered after transfer to the Republic of Korea even where the personal data transferred is pseudonymised.

3.1.1.2. Concept of personal information controller

53. Article 2(5) PIPA includes a definition of "personal information controller" meaning a public institution, legal person, organisation or individual, etc. that processes personal information directly or indirectly to operate personal information files "*as part of its activities*". However, in the additional safeguards set out in Notification No 2021-1, the term personal information controller is defined as a public institution, legal person, organisation, individual etc. that processes personal information directly or indirectly to operate the personal information files "*for business purposes*". Instead, footnote 272 of the draft decision states the following about the notion of personal information controller: "*As defined in Article 2 PIPA, i.e. a public institution, legal person, organisation, individual, etc. that processes personal information directly or indirectly to operate personal information files 'for official or business purposes'.*"

54. The EDPB acknowledges that these inconsistencies may be due to the translations of the original text as provided by the Korean authorities and invites the European Commission to verify the quality and certainty of the translations regularly. However, the EDPB stresses the fact that, in order to be able to assess the essential equivalence of the level of data protection of the Korean legal framework, a clear understanding of the processing purposes falling within the material scope PIPA is required. Further, in this context, the EDPB notes that the PIPA does not use the same terminology of the GDPR in relation to the notion of "controller" and "processor" and invites the European Commission to clarify the correct definition and scope of the concept of "personal information controller" and to specifically address whether this term also covers processors within the meaning of the GDPR, as this directly affects the scope of the adequacy decision[21].

3.1.2. Partial exemptions provided for in PIPA

55. Article 58(1) PIPA excludes the application of parts of PIPA (i.e., Articles 15 to 57) with respect to four categories of personal data processing as described below. Specifically, the exemptions relate to the provisions of PIPA on 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. However, the EDPB takes note that some general provisions of PIPA still remain applicable, such as those relating to the data protection principles (Article 3 PIPA) and individual rights (Article 4 PIPA). In addition, Article 58(4) PIPA sets out specific obligations on those four categories of data processing.

56. Firstly, the partial exemption covers personal information collected pursuant to the Statistics Act for processing by public institutions. The European Commission states in Recital 27 of its draft decision

[21] See also para. 38 above.

that 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. According to the draft decision, however, even in these situations, such data is normally not transferred from controllers/processors in the EEA but would rather be directly collected by public authorities in Korea.

57. The EDPB acknowledges the reasoning of the European Commission on the exceptionality of the application of the Statistics Act to the processing of personal data transferred under the adequacy decision; however, it would welcome further information and reassurances about the specific safeguards that would be applied in case personal data transferred from the EEA is further collected pursuant to the Statistics Act for processing by public institutions, in particular relating to the exercise of individual rights by data subjects in line with Article 89(2) GDPR in so far as such rights are not likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are not necessary for the fulfilment of those purposes.

58. In this perspective, the application of Article 4 PIPA also to this kind of processing appears to provide reassurances, however the EDPB would welcome additional information and clarifications in the adequacy decision on the specific obligations imposed, in accordance with Article 58(4) PIPA, on those processing activities, namely with respect to data minimisation, limited data retention, security measures and the handling of complaints.

59. Secondly, the partial exemption covers personal information collected or requested to be provided for the analysis of information related to national security. The EDPB is aware of the fact that in matters of national security, states have a broad margin of appreciation recognized by the ECtHR. The EDPB also notes that, according to Article 37(2) of the Korean Constitution, any restriction to the freedoms and rights, for example, when necessary for the protection of national security, may not violate the essential aspect of that freedom or right. Further, the EDPB notes the safeguards in Section 6 of Notification No 2021-1 regarding the processing of personal information for national security purposes including investigation of infringements and enforcement. However, in this context, the EDPB calls on the European Commission to clarify further the scope of the exemptions as it wonders whether all of the exemptions provided under Article 58(1) lit. 2 PIPA (Chapters III through VII) are relevant for the work of intelligence services, and whether they ensure equivalence with the necessity and proportionality principles. In particular, the EDPB invites the European Commission to provide more clarification regarding under which circumstances an intelligence service could rely on the exemptions. The EDPB considers it necessary to closely monitor the impact of these limitations in practice, especially on the effective exercise and enforcement of data subject rights.

60. Thirdly, the partial exemption applies to "*personal information processed temporarily where it is urgently necessary for public safety and security, public health, etc.*" According to Recital 29 of the European Commission's draft decision, this category is interpreted strictly by the PIPC and applies only in emergencies requiring urgent action, for example, to track infectious agents, or to rescue and aid victims of natural disasters.

61. The EDPB also emphasizes that any derogations to the level of protection for personal data should be interpreted strictly. At the same time, the EDPB notes that the provision is not strictly defined and does not provide an exhaustive list of examples of situations where the processing of personal information might be considered "*urgently necessary*". For example, the EDPB is concerned as to whether international transfers of health data during the ongoing COVID-19 pandemic would also fall within the scope of this exemption. In the light of above, the EDPB calls on the European Commission to provide further clarifications on the scope of this exemption and to fully monitor its application and scope to ensure that it does not lead to the level of protection of personal data from the EEA being lowered after transfer to Korea on the basis of the adequacy decision.

62. Finally, the partial exemption applies to personal information collected or used for the purposes of reporting by the press, missionary activities by religious organizations, and nomination of candidates by political parties[22]. With respect to the processing of personal information by the press for journalistic activities, the European Commission states in Recital 31 of its draft decision that 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 (hereafter "**Press Act**"), and presents specific safeguards that follow from the Press Act. The EDPB would, however, call on European Commission to fully monitor this exemption and the relevant case law in order to ensure that an equivalent level of data protection is ensured also in practice in the Korean legal framework.

3.1.3 Grounds for lawful and fair processing for legitimate purposes

63. According to the GDPR Adequacy Referential, in line with the GDPR, data must be processed in a lawful, fair and legitimate manner. The legal basis, under which personal data may be lawfully, fairly and legitimately processed should be set out in a sufficiently clear manner. The European framework acknowledges several such legitimate grounds including for example, provisions in national law, the consent of the data subject, performance of a contract or legitimate interests of the data controller or of a third party which does not override the interests of the individual.

64. Following a similar structure as the GDPR, PIPA first introduces the principle of lawfulness, fairness and transparency at the beginning (Article 3(1) and (2) PIPA), laying out the specific rules for its application later on (Articles 15 to 19 PIPA). Specifically, Article 15 PIPA includes a catalogue of legal grounds on which personal information controllers may base the collection of personal information and use it within the scope of the purpose collection. These legal grounds consist of (1) the data subject's informed consent; (2) statutory authorization or necessity for compliance with a legal obligation; (3) necessity for the performance of a public institution's duties; (4) necessity for the execution or performance of a contract with a data subject; (5) necessity for the protection of life, bodily or property interests of the data subject or a third party from imminent danger (and prior consent cannot be obtained); (6) necessity to attain a justifiable interest of a personal information controller which is superior to that of a data subject.

65. In addition, Article 17 PIPA lists the legal grounds applicable for sharing personal information with a third party which include (1) the data subject's informed consent; (2) statutory authorization or necessity for compliance with a legal obligation; (3) necessity for the performance of a public institution's duties; and (4) necessity for the protection of life, bodily or property interests of the data subject or a third party from imminent danger (and prior consent cannot be obtained). Even in the absence of the data subject's consent, the sharing of personal information is allowed where this occurs within the scope reasonably related to the purposes for which the personal information was initially collected (Article 17(4) PIPA).

66. Article 18 PIPA lays down specific rules for the use and sharing of personal information where this occurs out of the scope of the initial purpose of collection or provision. Among other, here too, consent is one such authorizing rule.

67. While acknowledging the substantial similarity of Korean law to the GDPR with respect to the principle of lawfulness and the existence of a general right to suspension (Article 37 PIPA), which can also be invoked where personal data is processed on the basis of consent, the EDPB would like to note the

[22] Accordingly, the processing of personal information by religious organisations for their missionary activities and the processing of personal information by political parties in the context of the nomination of candidates are also excluded from the scope of the adequacy decision. See also para. 37 above in section 2.3.2.

absence of a general right to withdraw consent under PIPA[23]. In light of the importance of consent as a legal ground in all of the above-described scenarios, and taking into consideration the role of individual rights in a data protection legal system for the purposes of safeguarding the data subjects' fundamental rights and freedoms, the EDPB invites the European Commission to further assess the impact of the lack of a general right to withdraw consent under Korean law and to provide further assurances to ensure that an essential level of data protection as the one provided for under the GDPR is guaranteed at all times also, where necessary, by clarifying the role of the right to suspension in this specific context.

3.1.4 The purpose limitation principle

68. The GDPR Adequacy Referential, in line with the GDPR, provides that personal data should be processed for a specific purpose and subsequently used only insofar as this is not incompatible with the purpose of the processing.

69. Pursuant to Article 3(1) and (2) PIPA, personal information controllers shall specify and explicit the purposes of processing and ensure that the processing is compatible with these purposes. While this principle is confirmed in other provisions (i.e., Articles 15(1), 18(1) and 19(1) PIPA), processing for "reasonably related" purposes is allowed in certain circumstances (see Article 17(4) PIPA)[24] as well as the out-of-purpose use and provision of personal information (see Articles 18 and 19 PIPA)[25].

70. The EDPB understands that in case of transfers of personal data from the EEA to the Republic of Korea on the basis of the adequacy decision, the purpose of collection of the EEA-based controllers constitutes the purpose for which the data is transferred applicable to the processing by the receiving Korean-based personal information controller. A change of purpose by the Korean-based controller would only be allowed as provided for in Article 18(2) lit. 1-3 PIPA, "*unless doing so is likely to unfairly infringe on the interest of a data subject or a third party*"[26]. In this context, the EDPB acknowledges the European Commission's statement in Recital 55 of the draft decision that, where changes of purpose are authorised by law, such laws have to respect the fundamental right to privacy and data protection. However, the EDPB notes that no specific information has been provided to sustain this particular statement, for example, no reference has been made to Article 37 of the (Korean) Constitution. Therefore, the EDPB calls on the European Commission to provide further assurances and guarantees in the draft decision to ensure that any laws authorizing a change of processing purpose are required to respect the fundamental rights and freedoms of data subjects to privacy and data protection.

3.1.5 The data quality and proportionality principle

71. The GDPR Adequacy Referential states that data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are processed.

---

[23] Even though data subjects may deny consent in certain circumstances, see for example Article 18(3) 5 PIPA. By contrast, the right to withdraw consent seems to exist only in specific cases ; pursuant to Article 27(1) 2 PIPA data subjects have the right to withdraw consent where they do not wish their personal information to be transferred to a third party owing to the transfer of some or all of the personal information controller's business, a merger, etc.; pursuant to Article 39(7) PIPA users may withdraw consent to the collection, use and provision of personal information at any time from information and communications service provider, etc.; and pursuant to Article 37 CIA an individual credit information subject may revoke the consent which had been provided to a credit information provider/user.

[24] Whereby purpose compatibility must be ascertained in advance on the basis of the criteria laid down in Article 14-2 PIPA Enforcement Decree.

[25] See also above under para. 66.

[26] Article 18(2) PIPA.

72. Under PIPA, personal information controllers must 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). Personal information controllers are required to collect as little personal information as necessary to achieve a given purpose. They bear the burden of proof in this regard (Article 16(1) PIPA).

73. Against this background, the EDPB shares the European Commission's assessment with respect to the essential equivalence of the level of protection under PIPA vis-à-vis the GDPR in this regard.

3.1.6 Data retention principle

74. According to the GDPR Adequacy Referential, as a general rule data should be kept for no longer than is necessary for the purposes for which the personal data is processed. As per Article 21(1) PIPA, this principle exists in Korean law as well. Under PIPA, personal information controllers are required to destroy personal information without delay when the personal information becomes unnecessary upon expiry of the retention period or upon achievement of the intended purpose of processing, unless statutory retention periods apply.

75. The EDPB is, however, concerned as to the fact that Article 21(1) PIPA is not applicable to pseudonymised personal information. The EDPB takes note of the fact that, according to Section 4(iii) of Notification No 2021-1, "[w]*here 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* [sic] *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*." Given, here too, the importance of Notification 2021-1 and with a view to having legal certainty as to the equivalence of the level of protection of personal data transferred to the Republic of Korea under the adequacy decision, the EDPB reiterates its call on the European Commission to provide further information specifically on how Notification No 2021-1 is made binding and its enforceability and validity is ensured[27].

3.1.7 The security and confidentiality principle

76. As described in the GDPR Adequacy Referential, the security and confidentiality principle requires data processing entities to make sure that personal data is processed in a manner that ensures its security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, by using appropriate technical or organisational measures. The level of the security should take into consideration the state of the art and the related costs.

77. The European Commission has identified a similar principle of data security in Article 3(4) PIPA, which is further specified in Article 29 PIPA. In addition, data security provisions apply where the personal information controller engages an "outsourcee". The security of the processing must be ensured through technical and managerial safeguards, which must also be included in the binding data processing agreement (Article 26 PIPA and Article 28 PIPA Enforcement Decree). Further, under PIPA specific obligations apply in the event of a data breach, including the obligation to notify affected data subjects and the supervisory authority where the number of affected data subjects exceeds the applicable threshold (Article 34 PIPA in conjunction with Article 39 PIPA Presidential Decree), except where the affected data is pseudonymised personal information processed for the purposes of

[27] See also above para. 51 under section 3.1.1.1 of this opinion, as well as para. 52 for the EDPB's general concerns regarding the impact of pseudonymisation under Korean law.

statistics, scientific research or archiving in the public interest (Article 28(7) PIPA). Here, too[28], the EDPB is concerned with the wide reaching exemptions for pseudonymised information and reiterates its call on the European Commission to further assess this aspect to ensure that a level of protection essentially equivalent is provided for under Korean law[29].

78. Notwithstanding, in sum, the EDPB is satisfied with the European Commission's assessment and conclusion regarding the essential equivalence of Korean law with respect to the principle of security and confidentiality.

3.1.8 The transparency principle

79. Based on Article 5(1)(a) GDPR, transparency is a fundamental principle of the EU data protection system. Recital 39 GDPR outlines the crucial function of this principle by stating that "[i]*t should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. (...) Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing.*"

80. The GDPR Adequacy Referential explicitly names "transparency" as one of the content principles to be taken into account when evaluating the essential equivalence of the level of protection provided for by a third country. More specifically, it states that "[e]*ach individual should be informed of all the main elements of the processing of his/her personal data in a clear, easily accessible, concise, transparent and intelligible form. Such information should include the purpose of the processing, the identity of the data controller, the rights made available to him/her and other information insofar as this is necessary to ensure fairness. Under certain conditions, some exceptions to this right for information can exist, such as for example, to safeguard criminal investigations, national security, judicial independence and judicial proceedings or other important objectives of general public interest as is the case with Article 23 GDPR.*"

81. Similarly as is the case with the GDPR, under PIPA a general transparency principle exits requiring personal information controllers to make public their privacy policy and other matters related to personal information processing (Article 3(5) PIPA). Specific information obligations apply where personal information controllers seek to obtain consent from the data subjects for the collection and processing of personal information (Article 15(2) PIPA), for the sharing of personal information with a third party (Article 17(2) PIPA) and for out-of-purpose processing (Article 18(3) PIPA). It is noteworthy that these information obligations also apply *mutatis mutandis* to the outsourcee (Article 26(7) PIPA).

82. The EDPB acknowledges and welcomes the additional safeguards in Section 3(i) and (ii) of Notification No 2021-1[30] relating to information to be provided to data subjects when their data are transferred by an EEA entity taking into account the fact that pursuant to Article 20(1) PIPA, when data has not been obtained from the data subject, data subjects are informed only upon request while a general right to be informed is only recognized pursuant to Article 20(2) PIPA where certain processing operations exceed thresholds set forth in the PIPA Enforcement Decree (Article 15(2)).

83. Overall, the EDPB is satisfied that the level of protection under Korean law with respect to the transparency principle is essentially equivalent to that provided under the GDPR.

[28] As already laid down in paras. 51-52 above and section 3.1.1.1 of this Opinion.
[29] See also sections 3.1.6 and 3.1.10 of this Opinion.
[30] Annex I of the draft decision.

3.1.9 Special categories of personal data

84. For a third country's data protection system to be recognized as providing a level of protection of personal data essentially equivalent to that of the GDPR, specific safeguards should exist where special categories of personal within the meaning of Articles 9 and 10 GDPR are involved.

85. Under PIPA, specific provisions apply to the processing of so-called sensitive information, which includes personal information revealing the ideology, belief, admission to or withdrawal from a trade union or political party, political opinions, health, sex life, and other personal information that is likely to markedly threaten the privacy of any data subject, as well as, by reference to the PIPA Enforcement Decree, DNA information acquired from genetic testing, data that constitutes a criminal history record; 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; and personal information revealing racial or ethnic origin.

86. Similarly to the GDPR, Korean data protection law prohibits the processing of sensitive information unless specific exemptions apply consisting of (1) informing the data subject and obtaining a specific consent and (2) legal provisions authorizing the processing (Article 23(2) PIPA).

87. On this basis, the EDPB in principle agrees with the European Commission's conclusion of essential equivalence of Korean law with respect to the processing of special categories of personal data. However, the EDPB would like to note that it has not been provided with the PIPA Handbook nor with the clarifications from the PIPC with regard to the term "sexual life" being interpreted as also covering the individual's sexual orientation or preferences, which have not been included in Notification No 2021-1. The EDPB therefore calls on the European Commission to provide this information to be able to independently assess it. Further, the EDPB invites the European Commission to specifically cite the documents where the information it refers to on this topic can be found.

3.1.10 Rights of access, rectification, erasure and objection

88. In the Korean legal framework, data subject rights are recognized in Article 3(5) PIPA – according to which the personal information 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 and, as for "personal credit information" (i.e., "credit information, that is information that is necessary to determine the creditworthiness of parties to financial or commercial transactions – see Recital 3 of the draft decision), in Articles 37, 38, 38(3) CIA.

89. The EDPB notes that the right of access (and of rectification and erasure which may be exercised by a "*data subject who has accessed his or her personal information pursuant to Article 35*" PIPA) may be limited or denied "*where access is prohibited or limited by Acts*", "*where access may cause damage to the life or body of a third party, or unjustified infringement of property and other interests of any other person*", and in addition, for public institutions, where granting access "*would cause grave difficulties*" in carrying out certain functions, further specified in Article 35(4) PIPA[31]. Similar provisions are also contained in Article 37 PIPA relating to the right of suspension of processing of personal information.

90. Article 23 GDPR allows Union or Member State law to restrict individual rights when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society and envisages such restrictions to safeguard, among others, the protection of the data subject or the rights and freedoms of others and "*a monitoring, inspection or*

[31] The same conditions and exceptions to the rights of access and correction envisaged by the PIPA apply also with regards to the right of access and correction envisaged for credit personal information by the CIA (footnote 135 of the draft decision).

regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g) of the same article".

91. Against this background, the EDPB would welcome general reassurances in the draft decision on the need for any law or statute limiting the rights of the data subjects to meet the requirements of the Korean 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 that this limitation may not affect the essence of the freedom or right concerned (Article 37(2) of the Korean Constitution).

92. Furthermore, with regard to the exception related to "*an unjustified infringement of property or other interests of any other persons*", the EDPB acknowledges that this "*implies that a balancing should take place between the constitutionally protected rights and freedoms of the individual, on the one hand, and of other persons, on the other hand*"[32], however, it would call on the European Commission to fully monitor the application of this exception and the relevant case law in order to ensure that an equivalent level of protection of data subject rights is ensured also in practice in the Korean legal framework.

93. By the same token, the EDPB would welcome an attentive monitoring of the application of the exception for the public bodies, in particular with regard to the cases where granting access would be considered as causing "*grave difficulties*" in performing their duties considering that this expression seems to be broader than the one used in other provisions of the PIPA, e.g. in Article 18(2) lit. 5[33], and should be interpreted restrictively in order to avoid unduly restrictions of the data subject rights.

94. Besides, the EDPB is concerned as to whether the exceptions according to which the provisions regarding transparency on request (Article 20 PIPA) and individual rights (Articles 35 to 37 PIPA) – as well as the similar ones relating to the requirements for information and communication service providers (Article 39(2), 39(6) to 39(8) PIPA) and those contained in the CIA (see exceptions envisaged by Article 40(3) CIA) – do not apply with respect to pseudonymised information, when this is processed for purposes of statistics, scientific research or archiving in the public interest (Article 28(7) PIPA) are in line with the safeguards provided for in the European legal framework.

95. These provisions seem to introduce a general derogation for such kind of processing while the GDPR envisages that, where personal data (including pseudonymised personal data) is processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the data subject rights but only "*in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes*", pseudonymisation being only one of the technical and organisational measures to be adopted to ensure respect for the principle of data minimization (Article 89(1) GDPR).

96. The European Commission considers the derogation envisaged by Article 28(7) PIPA to be justified also in light of Article 28(5) PIPA by which the personal information controller is expressly prohibited to process the pseudonymised information for the purpose of identifying a certain individual and refers to the approach of Article 11(2) GDPR (in conjunction with Recital 57 GDPR) for processing which does not require identification[34].

[32] Recital 76 of the draft decision.

[33] In relation to exceptions to the limitation to Out-of-Purpose Use and Provision of Personal Information, Article 18(2) lit. 5 PIPA refers to situations where, for public institutions, "*it is impossible*" to perform the duties.

[34] To be noted that the same reasoning would not be applicable as such to the exception envisaged by Article 40(3) CIA for the processing of pseudonymised credit information because Article 40(2)(6) envisages that: "*A credit information company, etc. shall not process pseudonymised information in a way that a specific individual*

97. Indeed, according to Article 11 GDPR, the controller shall not be obliged to "*maintain, acquire or process additional information in order to identify the data subject*" for the sole purpose of complying with the GDPR if, for the intended purposes, it may process personal data which do not or do no longer require the identification of a data subject; in such cases, when the controller is able to demonstrate that it is not in a position to identify the data subject, data subject rights do not apply. As acknowledged by the European Commission[35], the GDPR therefore requires, in such cases, a "practical" impossibility for the data controller and, in accordance with the principle of data minimization, recognizes that no additional data has to be processed "because of" the GDPR.

98. However, the EDPB deems this situation to be different from the one in which a controller is practically in a position to identify the data subject but it is not allowed to do so by a statutory provision such as the one contained in Article 28(5) PIPA. In this respect, the EDPB welcomes the clarifications provided by the PIPC in the Notification No 2021-1[36] confirming that Section 3 PIPA (including Article 28(7)) and the exception of Article 40(3) CIA only apply when pseudonymised information is processed for scientific research, statistics or archiving in the public interest. However – and additionally to the concerns already mentioned about the effective binding nature of the Notification No 2021-1[37], the EDPB still wonders whether the derogations envisaged by Articles 28(7) PIPA and Article 40(3) CIA could be considered as necessary and proportionate in a democratic society as far as they restrict the data subject rights in all cases where pseudonymised information is processed for such purposes – i.e., even when the personal information controller is practically in a position to identify the data subject and the rights are not likely to render impossible or seriously impair the achievement of the specific purposes.

99. In particular, the EDPB has concerns that these derogations would not be justified and would need to be further scrutinized especially if applied by the personal information controller that pseudonymises the data "*for statistical purposes, scientific research purposes, and archiving purposes in the public interest, etc.*", in accordance with Article 28(2) PIPA "*without the consent of data subjects*" (and without providing information envisaged by Article 20 PIPA)[38], as far as this controller maintains the information allowing the re-identification. Under the GDPR individuals should be able to exercise their rights with regard to any information which is able to identify or single them out, even if the information is considered "pseudonymised" unless the already mentioned Article 11 GDPR applies. In this respect, the EDPB notes that only when this data is provided to a third party for the same statistical, scientific research purposes and archiving purposes, information that may be used to identify a certain individual should not be included and therefore only the personal information controller to which pseudonymised data is provided according to Article 28-2(2) PIPA would probably be "practically" not in a position to identify the data subject without additional information.

100. In a nutshell, considering that, as recognized by the European Commission, "*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)*"[39]

---

may be identified for any profit-making or unfair purposes" and could therefore allow re-identification for a fair purpose such as the one to fulfil a data subject request.

[35] See Recital 82 of the draft decision.

[36] Section 4 of Annex I to the draft decision.

[37] See section 3.1.1.1 above.

[38] See Article 28(7) PIPA, as explained in the Notification No 2021-1, according to which certain safeguards contained in the PIPA, i.e., "*Articles 20, 21, 27, 34 (1), 35 through 37, 39(3), 39(4), 39(6) through 39(8)*", shall not apply to the pseudonymised information processed for the purpose of compiling statistics, scientific research, preservation of public records, etc.

[39] Recital 42 of the draft decision.

but it envisages for such cases important restrictions on the data subjects rights, the EDPB calls on the European Commission to assess further the derogations contained in Article 28(7) PIPA and Article 40(3) CIA and to attentively monitor their application and relevant case law[40] in order to ensure that the data subject rights will not be unduly restricted when personal data transferred under the adequacy decision is processed for these purposes taking into account that, in many cases, these rights help also the controller to ensure the quality of the processed data.

3.1.11 Restrictions on onward transfers

101. The GDPR Adequacy Referential clarifies that the level of protection of natural persons whose personal data is transferred under an adequacy decision must not be undermined by the onward transfer and therefore any onward transfer "*should be permitted only where the further recipient (i.e., the recipient of the onward transfer) is also subject to rules (including contractual rules) affording an adequate level of protection and following the relevant instructions when processing data on the behalf of the data controller*".

102. As for the onward transfers to outsourcees (i.e., "processors") established in other third countries, the EDPB takes note that no special rules are in place in the Korean legal framework to cover these cases and that, as considered by the European Commission[41], a Korean personal information controller has to ensure compliance with PIPA's provisions on outsourcing (Article 26 PIPA) by means of a legally binding instrument and it will be responsible for the personal information that has been outsourced (Article 26 PIPA).

103. With regards to onward transfers to third parties (i.e., other personal information controllers), according to Article 17(3) PIPA, a Korean personal information controller has to inform the data subjects about and obtain their consent for the overseas transfers and it "*shall not enter into a contract for the cross-border transfer of personal information in violation of the PIPA*". The EDPB notes that this last provision will ensure – as considered by the European Commission[42] – that no contract for cross-border transfers could contain obligations contradicting the requirements imposed by PIPA on the personal information controller and could be therefore considered as a safeguard, however, it does not impose any obligation to put in place safeguards to ensure that the same level of protection afforded by the PIPA will be afforded by the recipient. Therefore, the EDPB acknowledges that informed consent of the data subject will generally be used as a basis for data transfers from a Korean-based personal information controller to a third country-based recipient.

104. In this regard, the additional clarifications provided by the PIPC in Notification No 2021-1 regarding the obligation to inform individuals about the third country to which their data will be provided[43] are welcomed as this – as highlighted by the European Commission[44] – would help data subjects in the EEA take a fully informed decision on whether or not to consent to an overseas provision.

105. However, as also considered in the Opinion 28/2018 regarding the European Commission Draft Implementing Decision on the adequate protection of personal data in Japan, it has to be highlighted that, under the GDPR, data subjects have to be explicitly informed about the possible risks of such transfers arising from the absence of adequate protection in the third country and the absence of appropriate safeguards prior to consent. Such notice should include for example information that there might not be a supervisory authority and/or data processing principles and/or data subject rights

[40] See, for example, the Open Net's constitutional challenges (information at https://opennet.or.kr/19909 available in Korean only).
[41] Recital 87 of the draft decision.
[42] Recital 88 of the draft decision.
[43] Ibid.
[44] Ibid.

in the third country[45]. For the EDPB, the provision of this information is essential in order to enable the data subject to give an informed consent with full knowledge of these specific facts of the transfer[46]. The EDPB, therefore, has concerns with the European Commission's findings in the draft adequacy decision vis-à-vis this specific kind of transfers. Data subjects are usually not knowledgeable about the data protection framework in third countries. Hence, it cannot be concluded that a data subject could assess the risk of a transfer by only knowing the specific country of destination. There rather has to be a clear information about the specific risks of such a transfer of personal data to a country outside the territory of the Republic of Korea prior to the data subject's consent.

106. Thus, the EDPB invites the European Commission to ensure that the information to be provided to the data subject "*on the circumstances surrounding the transfer*" includes information on the possible risks of the transfer arising from the absence of adequate protection in the third country and of appropriate safeguards. This is important for the EDPB in order to assess whether the consent requirements are essentially equivalent to the GDPR.

107. Furthermore, considering that consent needs to be freely given, informed, specific and unambiguous, the EDPB would welcome reassurances in the adequacy decision that personal data will not be transferred from Korean personal information controllers to a third party in a third country in any situation in which under the GDPR valid consent could not be provided, e.g. because of an imbalance of power.

108. In relation to cases where the personal information controller may provide personal information to a third party overseas without the data subject's consent – i.e., (1) if personal information is provided within the scope reasonably related to the initial purpose of collection according to Article 17(4) PIPA; and (2) if personal information can be provided to a third party in exceptional cases mentioned in Article 18(2) PIPA – the EDPB takes note of the clarifications provided by the PIPC in Section 2 of Notification No 2021-1 (and welcomes the envisaged duty imposed on the Korean-based controller and the overseas recipient to ensure, through a legally binding instrument (such as a contract), a level of protection equivalent to PIPA, including with respect to data subject rights).

3.1.12 Direct marketing

109. According to Articles 21(2) and 21(3) GDPR and the GDPR Adequacy Referential, the data subject has always to be in a position to object without any charge to data processing for purposes of profiling and direct marketing.

110. With regard to the right to suspension envisaged by Article 37 PIPA, the EDPB acknowledges that the European Commission considers that this right also applies where data is used for direct marketing purposes[47]. However, the EDPB would welcome additional information and clarifications in the draft decision in relation to this assessment and, in particular, on the practical application of the right to suspension in the context of direct marketing (e.g. references to relevant case law, etc.). In this respect, the EDPB would also highlight that the right to ask a credit information provider/user to stop contacting him/her for the purpose of introducing or soliciting the purchase of goods or services is explicitly set forth by the CIA (Article 37(2)).

111. Furthermore, as recognized by the European Commission[48], in the Korean legal framework such processing generally requires the specific (additional) consent of the data subject (see Article 15(1) lit. 1, Article 17(2) lit. 1 of PIPA).

[45] EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25 May 2018, p.8.
[46] EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25 May 2018, p.7.
[47] Recital 79 of the draft decision.
[48] Ibid.

112. As it cannot be ruled out that personal data transferred from the EEA may be processed in Korea for such purposes, the EDPB would also welcome clarifications in the adequacy decision on the existence of the right for a data subject to withdraw consent[49] and on the right to have his or her personal data erased and no longer processed where the processing is based on consent (such as in case of processing carried out for marketing purposes) and the data subject has withdrawn it.

3.1.13 Automated decision-making and profiling

113. As acknowledged by the European Commission in its draft decision[50], 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. Still, the Korean legal system envisages such right in the CIA which contains rules on automated decisions (Article 36(2)) even if their application seem to be out of the scope of PIPC supervision (and, as such, out of the scope of application of this draft decision – see section 2.3.2 above on the scope of application of the draft decision).

114. As already considered by the Article 29 Working Party[51] in its opinion 1/2016 on the Privacy Shield and by the EDPB in its previous opinion on the adequacy decision relating to Japan[52], the growing importance of automated decision-making, profiling and A.I. would suggest taking a more protective approach in this regard. Contrary to the European Commission's arguments[53] according to which the absence of specific rules on automated decision-making in the PIPA is unlikely to affect the level of protection as regards personal data that has been collected in the Union (since any decision based on automated processing would typically be taken by the controller in the Union which has a direct relationship with the concerned data subject), the EDPB considers that it cannot be ruled out that automated decision-making could be used by a Korean-based personal information controller in case of data transferred under the adequacy decision (for instance, in the context of employment, for assessing performance at work, reliability, conduct, etc.).

115. Developing new technologies enable companies to more easily implement or consider the implementation of automated decision-making systems which may lead to weakening the position of individuals. Where decisions made solely by those automated systems impact upon the legal situation of individuals or significantly affect them (for example, by black-listing and thereby depriving individuals of their rights) it is crucial to provide for sufficient safeguards including the right to be informed about the specific reasons underlying the decision and the logic involved, to correct inaccurate or incomplete information, and to contest the decision where it has been adopted on an incorrect factual basis[54].

116. In this context, the EDPB has concerns regarding the lack of legal provisions on automated decision-making in the PIPA and therefore invites the European Commission to address this concern and keep monitoring the development of the Korean legislative framework in this respect.

[49] See also above under para. 67: While the possibility to revoke consent is clearly envisaged in Article 37(1) CIA, this right is only mentioned twice in PIPA for specific circumstances in Articles 27(1)2 and Article 39(7).
[50] See Recital 81 of the draft decision.
[51] This Working Party was set up under Article 29 of Directive 95/46/EC. It was an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. The WP29 has now become the EDPB.
[52] Opinion 28/2018 regarding the European Commission Draft Implementing Decision on the adequate protection of personal data in Japan adopted on 5 December 2018.
[53] Recital 81 of the draft decision.
[54] WP 254, p. 7.

3.1.14 Accountability

117. The Korean legal framework contains several rules aimed at ensuring that personal information controllers put in place appropriate technical and organisational measures to effectively comply with their data protection obligations and be able to demonstrate such compliance, among other to the competent supervisory authority. In particular, the EDPB welcomes the existence of rules envisaging the adoption of an internal management plan (Article 29 PIPA), the obligation of carrying out a so-called privacy impact assessment ("**PIA**") for cases where processing presents a higher risk of possible privacy violations (Article 33(1) PIPA and Article 35 PIPA Enforcement Decree), rules on training and supervision of staff (Article 28 PIPA) as well as the obligation to designate a privacy officer (Article 31 PIPA in conjunction with Article 32 PIPA Enforcement Decree).

118. The EDPB shares the view of the European Commission relating to the essentially equivalent protection they ensure – even in cases where the rules seem to relatively diverge from the ones envisaged by the GDPR, e.g. there is no provision stating the need for the privacy officer to be independent, however, it is clearly set forth that he/she has to report to the management of the personal information controller (Article 31(4) PIPA) and that he/she must not suffer unjustified disadvantages as a consequence of performing these functions (Article 31(5) PIPA) – and would suggest the European Commission monitoring, when reviewing the adequacy decision, the actual application of these provisions in order to assess their effective implementation.

3.2. Procedural and Enforcement Mechanisms

119. Based on the criteria set forth in the GDPR Adequacy Referential, the EDPB has analysed the following aspects of the Korean data protection framework as covered under the draft decision: the existence and effective functioning of an independent supervisory authority; the existence of a system ensuring a good level of compliance and a system of access to appropriate redress mechanisms equipping individuals in the EEA with the means to exercise their rights and seek redress without encountering cumbersome barriers to administrative and judicial redress.

120. In accordance with Chapter VI of the GDPR, and Chapter 3 of the GDPR Adequacy Referential one or more independent supervisory authorities must exist, tasked with monitoring, ensuring, and enforcing compliance with data protection and privacy provisions in a third country to ensure an EEA equivalent level of protection.

121. In this context, the third country supervisory authority must act with complete independence and impartiality in performing its duties and exercising its powers and in doing so shall neither seek nor accept instructions. In addition, the supervisory authority should have all the necessary and available powers and missions to ensure compliance with data protection rights and promote awareness. Consideration should also be given to the staff and budget of the supervisory authority. The supervisory authority shall also be able to start proceedings, on its own initiative.

3.2.1 Competent Independent Supervisory Authority

122. In the Republic of Korea, the independent authority in charge of monitoring and enforcing the PIPA is the PIPC. The PIPC consists of one 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 upon recommendation of the Chairperson, two upon recommendation by representatives from the political party to which the President belongs and the three remaining members upon recommendation by representatives from other political parties (Article 7(2)(2) 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).

123. In this sense, the EDPB acknowledges that despite its recent reorganisation which deeply amended its status and powers, the PIPC has put considerable efforts into building the required infrastructure to accommodate the implementation of the PIPA and its most recent amendments. Among these efforts, reference can be made to the establishment of the PIPC's rules, the elaboration of guidelines to give guidance on the interpretation of the PIPA, and the setting up of a helpline to advise business operators and individuals on data protection provisions as well as a mediation service to handle complaints. 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[55].

124. The appointment and composition of the PIPC are set forth in Article 7(2) PIPA. Although the PIPC falls within the jurisdiction of the Prime Minister (and the Chairperson and Vice Chairperson are appointed by the President upon the recommendation of the Prime Minister), the legal framework mandates that the Commissioners perform their duties independently, according to law and their conscience. The EDPB acknowledges the institutional and procedural safeguards contained in the PIPA and in particular in Articles 7(4) to 7(7). Still, the EDPB would welcome the European Commission to monitor any developments that might affect the independence of the members of the South Korean supervisory authority.

125. Moreover, the draft decision does not yet comprise an analysis of the PIPC's budget, including sources of funding and budget transparency. The EDPB considers that this element, which is mentioned in both, Article 56(1) GDPR and the procedural and enforcement data protection principles and mechanisms to be considered under the GDPR Adequacy Referential when evaluating a country's or an international organization's system, must be thoroughly taken into account as it is an indicator of the economic and human resources available to the supervisory authority to perform its data protection statutory obligations and tasks independently, and would therefore advise the European Commission to account for it in more detail in the draft decision.

3.2.2. Existence of a data protection system ensuring a good level of compliance

126. In the field of enforcement, the EDPB acknowledges the range of enforcement powers and sanctions of the PIPC as provided for in the PIPA and the CIA and takes note of the clarifications contained in Notification No 2021-1 according to which the conditions referred to in Articles 64(1) PIPA and Article 45(4) CIA[56] will be applicable whenever any of the principles, rights and duties, included in the law to protect personal information, are violated. However, it would recommend the European Commission to closely monitor the application in practice of the PIPC's powers to order the violator to take the measure it deems to be appropriate under the ones listed in Article 64(1) or Article 45(4) CIA.

127. Furthermore, regarding the corrective measures provided in Article 64(1) PIPA, in case of failure to comply with a corrective measure, the PIPC is empowered to impose a fine of a maximum amount of 50 million Korean won (Article 75(2) lit. 13 PIPA). This amount is the equivalent of EUR 36,564. The EDPB considers and has concerns that such limited range of pecuniary sanctions might not have a particularly strong deterrent effect on violators as intended by the law in order to ensure the enforcement of data protection rules since it does not seem appropriately sufficient to dissuade, especially in the case of large organizations or undertakings with significant financial resources.

[55] The tasks and powers of the PIPC are mainly provided for in Articles 7(8) and 7(9), as well as in Articles 61 to 66 PIPA.

[56] I.e., "*a violation of the law is deemed to be likely to infringe on the rights and freedom of individuals in regard to personal information and failure to take action is likely to cause damage that is difficult to remedy*".

128. With respect to the possibility that the PIPC may demand that the head of a central administrative agency investigates the personal information controller or jointly engages in an investigation into violations of PIPA and even impose corrective measures with respect to personal information controllers under their jurisdiction (Article 63(4)-(5) PIPA), the EDPB notes that, even though some information has been provided in Recital 122 of the draft decision, overall the nature of these other agencies and their legal relations with the PIPC remains rather unclear. Additionally, Article 68(1) PIPA refers to many entities to which it would be possible to delegate the authority of the PIPC. Even if it seems that this provision has been applied only in relation to the Korean Internet and Security Agency[57], the EDPB would welcome clarifications with regards to the nature of the possible interactions between these entities and an attentive monitoring of the application of this provision in the future in order to ensure the independence of the entities tasked with applying the data protection rules.

129. With regard to sanctions, the Korean system seems to combine different types of sanctions, from corrective measures and administrative fines to criminal sanctions, which are likely to have a strong deterrent effect, and the Korean authorities presented several examples of fines imposed recently by the PIPC, *inter alia* one of 6.7 billion Korean won imposed in December 2020 on a company for violating different provisions of PIPA, and another fine of 103.3 million Korean won on 28 April 2021 issued to an AI Technology company for violating the rules of lawfulness of processing, in particular consent, and the processing of pseudonymised information.

130. Although the above-mentioned amounts may have a dissuasive effect, the EDPB would welcome additional information on the method used by the PIPC to calculate the level of administrative fines, for example with respect to fines imposed for a failure to comply with a corrective measure issued pursuant to Article 64(1) PIPA (see Article 75(2) lit. 13 PIPA). This is especially relevant concerning criminal sanctions and the application of the (Korean) Criminal Act.

3.2.3. The data protection system must provide support and help to data subjects in the exercise of their rights and appropriate redress mechanisms

131. Concerning redress, the Korean system seems to offer various avenues to ensure adequate protection and, in particular, the enforcement of individual rights with an effective administrative and judicial redress, including compensation for damages.

132. The Korean system also offers alternative mechanisms to which individuals can turn to obtain redress, in addition to administrative and judicial avenues, as explained in Recitals 132 and 133 of the draft decision, relating to the Privacy Call Centre and the Dispute Mediation Committee respectively. As these are additional redress avenues, the EDPB would welcome more detailed explanations on how they complement the redress possibilities before the PIPC and courts for the data subjects whose personal data is transferred to Korea under the adequacy decision.

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

133. With regard to the assessment of the level of data protection in the areas of law enforcement and national security, the European Commission provided comprehensive information in its draft decision and the annexes made available. Therefore, the EDPB refrains from reproducing most of the factual findings and assessments in this opinion.

[57] See Recital 117 of the draft decision and Article 62 Enforcement Decree.

134. The European Commission comes to the conclusion that in the above-mentioned areas a level of data protection exists that corresponds to the requirements set by the case law of the CJEU and can therefore be considered essentially equivalent to that of the European Union.

135. As a general remark, the EDPB would like to emphasize that even in cases where it seems or is claimed by the European Commission that data transferred from the EU to South Korea is unlikely to be affected by the relevant Korean law, it is still in order to assess the adequacy of the Korean level of data protection with regard to such cases. Their relevance is also demonstrated by the fact that the European Commission itself has addressed them in the draft decision.

4.1 General data protection framework in the context of government access

136. When it comes to access to personal data by public authorities, various Korean laws have to be looked at in order to assess the level of protection of the right to privacy and data protection. First of all, the EDPB notes that PIPA, as a key data protection law, claims broad applicability. However, while PIPA is fully applicable to the area of law enforcement, its application to data processing for national security purposes is limited. Pursuant to Article 58(1) lit.2 PIPA, Chapters III through VII do not apply to the processing of personal data for national security purposes. Yet, Chapters I, II, IX and X remain applicable for the area of national security. Thus, PIPA's core principles as well as the fundamental guarantees for data subject rights and the provisions on supervision, enforcement and remedies do apply to the access and use of personal data by national security authorities.

137. The South Korean constitution too enshrines essential data protection principles, namely the principles of legality, necessity and proportionality. These principles are also applicable to the access to personal data by South Korean public authorities in the areas of law enforcement and national security[58].

138. In the area of law enforcement the police, prosecutors, courts and other public bodies may collect personal data based on specific legislation, i.e. the Criminal Procedure Act ("**CPA**"), the Communications Privacy Protection Act ("**CPPA**"), the Telecommunications Business Act ("**TBA**") and the Act on Reporting and Using Specified Financial Transaction Information ("**ARUSFTI**"), which applies to the prosecution and prevention of money laundering and terrorist financing. These particular laws set out further limitations, safeguards and exemptions.

139. In the area of national security, based on the National Intelligence Service Act ("**NISA**") and further "national security laws"[59], the National Intelligence Service ("**NIS**") may collect personal data and intercept communications. In conducting its powers the EDPB understands that the NIS has to comply with the aforementioned legal provisions as well as with PIPA.

140. The EDPB asks the Commission to clarify whether there are other authorities in Korea besides the NIS that are responsible for the area of national security as in Annex I, Section 6 the European Commission gives the impression of the NIS as an example for national security agencies.

4.2 Protection and safeguards for communication confirmation data in the context of government access for law enforcement purposes

141. On the basis of the relevant law, the CPPA, law enforcement authorities may take two types of measures for access to communication information. The CPPA distinguishes between communication-restricting measures, which cover both the collection of the content of ordinary mail and the direct

[58] See Recital 145 of the draft decision.

[59] 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.

interception of the content of telecommunications[60], and the collection of so-called communication confirmation data. The latter include 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[61].

142. The EDPB notes that communication confirmation data seem not to benefit from the same safeguards as data collected via communication-restricting measures, i.e. content data. Indeed, the EDPB notices that the collection of content benefits from more safeguards than the collection of communication confirmation data for law enforcement purposes: First, unlike the collection of content data, the collection of communication confirmation data is not limited to the investigation of certain serious crimes, but can be performed when deemed necessary to conduct "any investigation or to execute any punishment" (Article 13(1) CPPA). Second, the collection of communication confirmation data is in principle not structured as a measure of last resort and only to be used where it is difficult to otherwise prevent the commission of a crime, arrest the criminal or collect evidence[62]. Communication confirmation data can be collected whenever a prosecutor or judicial police officer "deems it necessary" for investigating a crime or executing a punishment. However, an exception exists in this regard for real-time tracking data and communication confirmation data concerning a specific base station according to Article 13(2) CPPA. Third, law enforcement agencies collecting the content of communication must immediately cease to do so once continued access is no longer deemed to be necessary[63]. With regard to communication confirmation data, this is at least not explicitly stipulated in the CPPA or its Enforcement Decree.

143. The EDPB takes note that the collection of communication confirmation data may only take place on the basis of a court-issued warrant. Moreover, the CPPA requires detailed information to be provided both in the application for the warrant and in the warrant itself[64]. Such prior judicial authorisation serves to limit the law enforcement authorities' discretion in applying the law and to verify whether sufficient reasons for collecting communication confirmation data exist in each case. The EDPB also recognises that the law of the Republic of Korea does not seem to provide for general and indiscriminate retention of communication confirmation data. Thus, government access to such data always relates to data that is still retained for the purposes of billing and providing the communication services themselves.

144. However, the EDPB stresses that the CJEU has questioned the fact that traffic data are less sensitive than others, and in particular than content data[65]. Taking into account that communication confirmation data is afforded a lower level of protection than content data in several respects, the EDPB invites the European Commission to closely monitor whether the safeguards provided under Korean law for such category of personal data ensure an essentially equivalent level of protection to

[60] Articles, 3(2), 2(6), 2(7) CPPA.
[61] Article 2(11) CPPA.
[62] This is the case for content data according to Articles 3(2) and 5(1) CPPA.
[63] Article 2 CPPA Enforcement Decree.
[64] See Recital 156 of the draft decision.
[65] See CJEU, C-623/17, *Privacy International*, 6 October 2020, ECLI:EU:C:2020:790, para. 71: "*The interference with the right enshrined in Article 7 of the Charter entailed by the transmission of traffic data and location data to the security and intelligence agencies must be regarded as being particularly serious, bearing in mind inter alia the sensitive nature of the information which that data may provide and, in particular, the possibility of establishing a profile of the persons concerned on the basis of that data, such information being no less sensitive than the actual content of communications. In addition, it is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance (see, by analogy, judgments of 8 April 2014, Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 27 and 37, and of 21 December 2016, Tele2, C-203/15 and C-698/15, EU:C:2016:970, paragraphs 99 and 100)*."

the one guaranteed in the EU, in particular with regard to proportionality and foreseeability of the law.

4.3 Access to communication information by Korean public authorities for national security purposes

145. With regard to the legal framework for access of national security authorities to communication information transferred from the EEA to Korea, the EDPB has identified two points of concern, both of which relate to the regime of access to communications between non-Korean nationals that fall within a specific set of use cases (see paragraph 29). In those cases, with respect to both communication confirmation data and content data, certain safeguards otherwise provided are not applicable. In other words, in these specific cases, these data do not benefit from the same safeguards as data communicated when at least one Korean national is involved in the communication.

4.3.1 No obligation to notify individuals of government access to communications between foreign nationals

146. In a scenario as outlined above, i.e. where none of the parties of a communication is a Korean national, national security authorities are not obliged to notify individuals about the collection and processing of their data. The EDPB recognises that this issue affects only certain cases. Firstly, as already pointed out, whenever at least one Korean national is involved in a communication, the notification requirements according to the CPPA apply to all parties of the communication irrespective of their nationality[66]. Secondly, the collection of personal data stemming from communications exclusively between foreign nationals is subject to a specific set of use cases. In particular, the right to access in such cases extends to communications of a) countries hostile to the Republic of Korea, b) foreign agencies, groups or nationals suspected of engaging in anti-Korean activities[67], 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. Communications between EU individuals transferred from the EEA to Korea can thus only be collected for national security purposes if they fall within one of the three above-mentioned categories[68]. As a further limiting factor, the EDPB understood from the additional explanations of the European Commission that the applicable legal framework does not provide for the interception of data in transit outside of Korea.

147. Hence, the criticality of the lack of a notification requirement might, in terms of its practical impacts, be considered as limited. However, the EDPB stresses the importance of the (subsequent) notification of government access, in particular with regard to ensuring effective remedies. According to the CJEU, notification is "*necessary to enable the persons affected to exercise their rights under Articles 7 and 8 of the Charter to request access to their personal data that has been the subject of those measures and, where appropriate, to have the latter rectified or erased, as well as to avail themselves, in accordance with the first paragraph of Article 47 of the Charter, of an effective remedy before a tribunal*"[69]. Government access for purposes of national security oftentimes includes secret surveillance measures, meaning that the objects of the surveillance, the data subjects, are not aware of the processing of their data. Thus, there "*is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his knowledge and thus able to challenge their legality retrospectively or, in the alternative, unless any person who suspects*

[66] See Recital 192 of the draft decision.
[67] See Annex II, footnote 244, according to which the notion of anti-Korean activities refers to activities that threaten the nation's existence and safety, democratic order or the people's survival and freedom.
[68] See Recital 187 of the draft decision.
[69] CJEU, joined cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and others*, 6 October 2020, ECLI:EU:C:2020:791, para. 190.

that his communications are being or have been intercepted can apply to courts, so that the courts' jurisdiction does not depend on notification to the interception subject that there has been an interception of his communications"[70]. In this context and consistent herewith, the EDPB has many times expressed its concern with effective remedies in surveillance cases. The EDPB emphasises that the secrecy of government measures must not result in such measures being effectively unchallengeable. Against this background, whether or not the lack of a notification requirement for communications between foreign nationals impacts the level of data protection as assessed in the draft decision has to be evaluated as part of an overall assessment with special regard to the oversight and redress mechanisms provided under Korean law (see sections 4.7 and 4.8).

148. In addition, the EDPB notes in this context that the law refers to rather broad terms such as anti-Korean or antinational activities[71] and that it is difficult to foresee how these concepts are construed under Korean law. The EDPB invites the European Commission to monitor how these terms are fleshed out in Korean law and whether their application in practice meets the requirements of proportionality following from EU law.

4.3.2 No prior independent authorisation for collection of communication information between foreign nationals

149. In cases where EEA personal data derived from communications between non-Korean nationals (and falling within one of the abovementioned use cases) are to be processed in Korea for national security purposes, the collection of such data is not subject to prior approval by an independent body (as is the case for communications where at least one of the individuals concerned is a Korean national).[72]

150. Especially in light of the recent decisions of the European Court of Human Rights ("**ECtHR**") "Big Brother Watch and Others v. UK" and "Centrum för Rättvisa v. Sweden", the EDPB considers it necessary to explore whether this constitutes a critical shortcoming of the Korean data protection framework. In this regard, the EDPB recalls that, as underlined in its updated recommendations on the European essential guarantees for surveillances measures,[73] Article 6(3) of the Treaty on the European Union establishes that the fundamental rights enshrined in the ECHR constitute general principles of EU law while, as the CJEU recalls in its jurisprudence, the latter does not constitute, as long as the European Union has not acceded to it, a legal instrument which has been formally incorporated into EU law[74]. Thus, the level of protection of fundamental rights required by Article 45 of the GDPR must be determined on the basis of the provisions of that regulation, read in the light of the fundamental rights enshrined in the Charter. This being said, according to Article 52(3) of the Charter the rights contained therein which correspond to rights guaranteed by the ECHR are to have the same meaning and scope as those laid down by that Convention. Consequently, the jurisprudence of the ECtHR concerning rights that are also foreseen in the Charter must be taken into account, as a

[70] ECtHR, *Big Brother Watch and others v. UK*, 25 May 2021, ECLI:CE:ECHR:2021:0525JUD005817013, para. 337 and ECtHR, *Case of Roman Zakharov v. Russia*, 4 December 2015, ECLI:CE:ECHR:2015:1204JUD004714306, para. 234.

[71] The European Commission has explained that, according to explanations from the Korean government, this refers to 'activities that threaten the nation's existence and safety, democratic order or the people's survival and freedom', see also footnote 319 of the draft adequacy decision.

[72] See Recital 190 of the draft decision.

[73] See EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, paras. 10, 11.

[74] See CJEU, C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd. and Maximilian Schrems*, 16 July 2020, ECLI:EU:C:2020:559 (hereinafter "*Schrems II*"), para. 98.

minimum threshold of protection to interpret corresponding rights in the Charter, i.e. to the extent that the Charter, as interpreted by the CJEU, does not provide for a higher level of protection[75].

151. The EDPB notes that, while prior (independent) approval of surveillance measures is deemed an important safeguard against arbitrariness, such approval cannot be derived from the jurisprudence of the CJEU as an absolute requirement for the proportionality of surveillance measures. However, the ECtHR has now explicitly established the requirement of ex ante independent authorisation for bulk interception[76]. While the draft decision does not explicitly say so, the EDPB understands that the legal framework of the Republic of Korea does not provide for bulk interception but only for targeted interception of telecommunications[77]. The European Commission has confirmed this understanding.

152. That being said, the above-mentioned decisions of the ECtHR, in line with the case law of the CJEU[78] and previous case law of the ECtHR[79], once again show the importance of comprehensive supervision by independent supervisory authorities. The EDPB emphasizes that independent oversight at all stages of the process of government access for law enforcement and national security purposes is an important safeguard against arbitrary surveillance measures and thus for the assessment of an adequate level of data protection. The guarantee of independence of the supervisory authorities within the meaning of Article 8(3) of the Charter is intended to ensure effective and reliable monitoring of compliance with the rules on the protection of individuals with regard to the processing of personal data. This applies in particular in circumstances where, due to the nature of secret surveillance, the individual is prevented from seeking review or from taking a direct part in any review proceedings prior or during the execution of the surveillance measure.

153. The lack of prior independent approval cannot in itself be considered as a substantial shortcoming in Korean law with respect to the assessment of an essentially equivalent level of data protection. The assessment of adequacy depends, again, on all the circumstances of the case, in particular on the effectiveness of ex post oversight and legal redress as provided for in the legal framework of Korea (see further sections 4.7 and 4.8).

4.4 Voluntary disclosures

154. According to Article 83(3) TBA, telecommunication service providers may voluntarily hand over so-called "subscriber data"[80] to national security and law enforcement authorities upon request. While the EDPB notes that cases involving personal data that have been transferred from the EEA to Korea are likely to be rare, they still need to be analysed in order to assess the level of data protection, as already mentioned above.

---

[75] See CJEU, joined cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and others*, 6 October 2020, para. 124.

[76] See ECtHR, *Big Brother Watch and others v. UK*, 25 May 2021, ECLI:CE:ECHR:2021:0525JUD005817013, para. 351: "Bulk interception should be subject to independent authorization at the outset", "bulk interception should be authorized by an independent body; that is, a body which is independent of the executive".

[77] Only Annex II, section 3.2 contains an explicit declaration for national security purposes when it is specified that the limitations and safeguards "*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*".

[78] See, for example, CJEU joined cases C-203/15 and C-698/15, *Tele2 Sverige AB and others*, ECLI:EU:C:2016:970.

[79] See, for example, ECtHR, *Case of Roman Zakharov v. Russia*, 4 December 2015, ECLI:CE:ECHR:2015:1204JUD004714306.

[80] Concerned datasets would be: 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 (used to identify the rightful user of computer systems or communication networks).

155. The EDPB understands that in these cases the data protection safeguards of PIPA apply and public authorities, as well as telecommunications providers, have to comply with these requirements[81] and that both can be held liable for any infringement of the rights and freedoms of the concerned data subjects[82]. Furthermore the EDPB understands that telecommunications providers are not required to comply with such requests.

156. However, with regard to the concept of access to subscriber data by national authorities for law enforcement as well as and in particular for national security purposes via "voluntary disclosure" of telecommunication business operators, there is a concern of increased risk to the rights and freedoms of data subjects, especially with regard to their right to information.

157. According to Article 58(1) lit.2 PIPA, the provisions of Chapter III through VII shall not apply to any personal information requested to be provided related to national security. In this respect, for example, the provisions of Article 18 (Limitation to Out-of-Purpose Use and Provision of Personal Information) and Article 20 (Notification on Sources, etc. of Personal Information Collected from Third Parties) of PIPA are not applicable to such requests. In cases where a request is made by a national security authority, this raises the question, on the one hand, of whether Article 58(1) lit. 2 also precludes the application of PIPA to telecommunications providers as well. On the other hand, the question arises whether the exclusion of the application of Article 20 PIPA in such cases also applies to the corresponding provision from Section 3 of Annex I (Notification for the data where personal data have not been obtained from the data subject (Article 20 of the Act)). If this were the case and if Article 58(1) lit. 2 also addressed telecommunications providers, there would be a risk, according to the available information, that there would be no legal obligation to inform the data subjects about the voluntary disclose.

158. The EDPB is therefore concerned about the effectiveness that the information requirements could be rendered ineffective, making it considerably more difficult for data subjects to assert their data protection rights especially with regard to judicial redress. In this respect, the EDPB invites the European Commission to clarify the scope of the relevant provisions.

4.5 Further use of information

159. The principle of purpose limitation is a core legal requirement of data protection. It requires that personal data is only to be collected for specified, explicit and legitimate purposes and not to be further processed in an incompatible way to those purposes. Furthermore public authorities are under EU law permitted to process personal data for the prevention, investigation or prosecution of criminal offenses even if those data were initially obtained for different purpose if these authorities have a legal basis to process such data under the relevant law and if the further processing is not disproportionate[83].

160. According to this the EDPB notes that the Korean data protection framework provides for similar safeguards and limitations to the ones provided under EU law in relation to the further use of the information collected for law enforcement and national security purposes, e.g. Article 3(1)-(2) PIPA principle of purpose limitation.

4.6 Onward transfers and intelligence sharing

161. Article 44 GDPR provides that transfers and onward transfers of personal data shall only take place if the level of protection guaranteed by the GDPR is not undermined. Thus, the level of protection afforded to personal data transferred from the EEA to Korea must not be undermined by the further

[81] See Recitals 164 and 194 of the draft decision.
[82] See Recital 166 of the draft decision.
[83] See Article 4(2) LED.

transfer to recipients in a third country, i.e. onward transfers should be permitted only where a continued level of protection essentially equivalent to the one provided under EU law is ensured. Consequently, when assessing whether a third country ensures an adequate level of data protection, the country's legal framework for onward transfers must be taken into account. This is undisputed and in line with the view of both the European Commission[84] and the EDPB.

162. In this context, the EDPB takes note that the ECtHR has in its recent decisions "Big Brother Watch and Others v. UK" and "Centrum för Rättvisa v. Sweden" provided guidance[85] regarding the data protection precautions to be observed in Contracting States when communicating personal data to other parties for law enforcement and national security purposes in bulk collection cases: "*First of all, the circumstances in which such a transfer may take place must be set out clearly in domestic law. Secondly, the transferring State must ensure that the receiving State, in handling the data, has in place safeguards capable of preventing abuse and disproportionate interference. In particular, the receiving State must guarantee the secure storage of the material and restrict its onward disclosure. […] Thirdly, heightened safeguards will be necessary when it is clear that material requiring special confidentiality – such as confidential journalistic material – is being transferred*."[86]

163. In applying these standards, the ECtHR found in "Centrum för Rättvisa v. Sweden" that the absence of any express legal requirement in the interception regime to assess the necessity and proportionality of intelligence sharing for its possible impact on the right to privacy constitutes a violation of Article 8 ECHR. The ECtHR criticised that, as a result of the level of generality of the law, intercept material could generally be sent abroad whenever this is considered to be in the national interest irrespective of whether the foreign recipient offers an acceptable minimum level of safeguards[87].

164. Acknowledging that the legal framework of South Korea does not allow for bulk interception, still in light of the implications of the jurisprudence of the ECtHR as outlined above, the EDPB considers that, in addition to the requirements stemming from EU law as interpreted by the CJEU, the ECtHR's line of arguments should be considered for assessing whether the legal framework for onward transfers to a third country provides for adequate data protection standards.

4.6.1 Applicable legal framework for onward transfers by law enforcement authorities

165. In regard to onward transfers by the competent authorities for law enforcement purposes, the EDPB understands from the explanations by the European Commission that the Section 2 of Annex I of the draft decision concerning the limitation of onward transfers is applicable, including when the transfer is made on the basis of a statute other than PIPA. According to this rule, "*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. To fulfil the requirements of 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*

[84] See Recital 84 et seq. of the draft decision.

[85] The following elements were established on the occasion of the cases *Big Brother Watch* and *Centrum för Rättvisa*, which concern bulk interception regimes. The requirement of precautions to be taken when communicating material to other parties was already part of the criteria developed by the ECtHR in the context of targeted interception and had not been further specified by the ECtHR (see *Big Brother Watch and Others v. UK*, para. 335, 362).

[86] ECtHR, *Big Brother Watch and others v. UK*, 25 May 2021, ECLI:CE:ECHR:2021:0525JUD005817013, para. 362.

[87] See ECtHR, *Centrum för Rättvisa v. Sweden*, 25 May 2021, ECLI:CE:ECHR:2021:0525JUD003525208, para. 326.

rights in legally binding documents such as contracts, even after personal information is transferred overseas"[88].

166. The EDPB welcomes this provision, which, assuming the adequacy of the level of data protection in Korea for this purpose, ensures the continuity of a level of protection as essentially afforded under EU law for onward transfers. The Commission has confirmed that the EDPB's understanding, namely that this section of Annex I applies to all onward transfers by the competent authorities for law enforcement purposes, is correct. However, the EDPB points out that it must be ensured that this regulation provides for a continued level of protection in practice as there may be uncertainty as to which contractual safeguards and obligations or other similar mechanisms can be used to achieve such a level of protection in case of processing for law enforcement purposes. In this regard, it should be additionally stated, for example, that personal data may only be shared with the relevant competent authorities in the third country.

167. Subject to the clarification requested above as to whether KOFIU is covered by the draft decision the EDPB notes that the official representation on government access[89] explains that, according to Article 8(1) of the ARUSFTI, the Commissioner of the KOFIU may provide foreign financial intelligence services with specified financial transaction information, if deemed necessary to achieve the purpose of the ARUSFTI[90]. Article 8 ARUSFTI itself does not provide for an obligation to determine whether and ensure that the foreign country offers adequate data protection safeguards. Annex II does not refer to the new section of Annex I in this regard. Therefore, the EDPB calls on the European Commission to clarify the interrelation of the relevant section of Annex I on the limitation of onward transfers and the legal basis for onward transfers according to the ARUSFTI.

4.6.2 Applicable legal framework for onward transfers for national security purposes

168. The draft decision does not contain any information on the legal framework for onward transfers in the field of national security. To this end, the EDPB understands that, unlike for law enforcement purposes, the Section 2 of Annex I is not applicable to onward transfers for national security purposes. Articles 17 and 18 of PIPA which are subject of the Annex I section in question are part of Chapter III of PIPA which in turn is not applicable to the processing of personal data for national security purposes (Article 58(1) PIPA).

169. However, the EDPB assumes that Korea may need to and does transmit personal data to foreign intelligence services for national security purposes, e.g. in order to cooperate on combatting cross-border threats to national security, to warn foreign governments about or to solicit their help in identifying such threats.

170. The EDPB understood that, in the view of the European Commission, onward transfers are sufficiently regulated in Korean law by the safeguards following from the overarching constitutional framework, in particular the principles of necessity and proportionality, as well as by the core data protection principles regulated in PIPA, such as lawfulness and fairness of processing, purpose limitation, data minimisation, security and the general obligations to prevent abuse and misuse of personal information.

171. The EDPB recognises and acknowledges the general applicability of these key (data protection) principles but raises concerns that these safeguards are being of a very general nature and do not

[88] Draft decision, Annex I, p. 7.
[89] See draft decision, Annex II.
[90] See draft decision, Annex II, section 2.2.3.2. While such an exchange may only take place subject to the condition that the foreign service may not use the information for any purpose other than the original purpose of disclosure, and in particular not for a criminal investigation or trial (Article 8(2) ARUSFTI), the Commissioner of the KOFIU may, in receipt of a request by a foreign country, give consent to the use of such data for criminal investigations or trials for criminal offenses with a prior consent of the Minister of Justice (Article 8(3) ARUSFTI).

specifically refer to or address, in a legal basis, the specific circumstances and conditions for onward transfers of EEA transferred data for national security purposes. While these general and overarching principles are broadly applicable, the EDPB questions whether this could be considered to meet the criteria of clear and precise rules and to sufficiently enshrine effective and enforceable safeguards. Especially where government access and processing of personal data is exercised in secret and the inferences that could be drawn from the data are particularly severe, it is essential to have clear, detailed rules. The law should indicate the scope of any discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection. In the *Schrems II* ruling, the CJEU recalls that a legal basis which permits interference with fundamental rights must, in order to satisfy the requirements of the principles of necessity and proportionality, itself define the scope of the limitation on the exercise of the right concerned and lay down clear and precise rules governing the scope and application of the measure in question and impose minimum safeguards[91]. The EDPB is therefore concerned that it is not sufficient that such safeguards are generally enshrined in higher-ranking law without specifically implementing the notion of e.g. proportionality in the respective legal basis itself.

172. These concerns are supported by the above-mentioned decision of the ECtHR, in which the court found that a general rule without any express requirement to assess necessity and proportionality or consider privacy concerns is not compatible with the right to privacy pursuant to Article 8 ECHR. In this regard, the EDPB notes that in the law of the case at stake (as well as in the law of Korea) overarching (constitutionally guaranteed) principles of necessity and proportionality do exist, e.g. according to the Charter and through the accession to the ECHR.

173. The EDPB invites the European Commission to clarify the legal basis, how and to what extent and under which specific conditions intelligence service agencies are obliged to consider privacy concerns and data protection safeguards prior to disclosing personal data for national security purposes to foreign partners. In case such obligation is derived directly from constitutional principles, the European Commission should further assess the requirements of preciseness and clarity of the relevant law and confirm that the general constitutional and data protection principles are appropriately applied and implemented.

4.6.3 International agreements

174. The EDPB notes that the European Commission did not consider, as part of its adequacy assessment, the existence of international agreements concluded between Korea and third countries or international organisations that may provide for specific provisions for the international transfer of personal data by law enforcement and/or intelligence services to third countries. The EDPB considers that the conclusion of bilateral or multilateral agreements with third countries for the purposes of law enforcement or intelligence cooperation are likely to affect the data protection legal framework of Korea as assessed.

175. The EDPB therefore invites the European Commission to clarify whether such agreements exist, under which conditions they may be concluded and assess whether the provisions of international agreements may affect the level of protection afforded to personal data transferred from the EEA to Korea by the legislative framework and practices in relation to overseas disclosures for law enforcement and national security purposes.

4.7 Oversight

176. The EDPB notes that the oversight of criminal law enforcement as well as national security authorities is ensured by a combination of different internal and external bodies.

[91] See *Schrems II*, paras. 175 and 180.

177. In this context, it is to be noted that the CJEU has repeatedly stressed the need for independent oversight as an essential component of the protection of natural persons with regard to the processing of their personal data. The concept of independence encompasses the areas of institutional autonomy, freedom from instructions and material independence. In order to ensure a consistent monitoring and enforcement of data protection law, supervisory authorities must have effective powers, including corrective and remedial powers.

178. The EDPB agrees with the conclusion of the European Commission that, in an overall assessment, Korea can be considered to have an independent and effective supervisory system even though several bodies of the supervisory system do not meet the above requirements in themselves. For example, most of them do not have executive powers, but are limited to mere recommendations, e.g. the National Human Rights Commission or the Board of Audits and Inspections. Furthermore, most of the respective public bodies are not exclusively data protection institutions, but are usually entrusted with other tasks in the area of fundamental rights protection.

179. However, according to the European Commission's explanations, the EDPB notes that the supervision of law enforcement authorities is comprehensively and without exception guaranteed by the PIPC. Therefore the PIPC possesses investigative, remedial and enforcement powers under PIPA and other data protection laws (e.g. the CPPA) which apply to the entire area of access to personal data by law enforcement and national security authorities.

180. In this context, the EDPB would like to emphasize once again that in order to exercise their tasks and powers, supervisory authorities need to be equipped with sufficient human, technical and financial resources. In this regard, there is unfortunately a lack of any information on the designated supervisory bodies, in particular the PIPC. Therefore, the EDPB repeats its request to the European Commission to provide further information on the matter.

181. Overall, the EDPB would like to note that there are hardly any statements, examples or figures in the draft decision regarding the supervisory activities as well as the legal enforcement of data protection law by the supervisory bodies in the area of law enforcement and national security. These would be helpful in the context of evaluating the effectiveness of the supervisory bodies.

4.8 Judicial remedy and redress

182. The EDPB recalls that it is essential for an adequate level of data protection that data subjects are provided with comprehensive remedies and redress against unauthorized data access or processing. These legal remedies must be sufficient to enable the data subject to obtain access to the data stored about him or her and to request that it be corrected or deleted.

183. In the light of the *Schrems I* and *Schrems II* judgments by the CJEU, it is clear that in addition to the right to turn to competent authorities, effective judicial protection in the meaning of Article 47(1) of the Charter is of fundamental importance for the assumption of adequacy of the law of a third country.

184. The EDPB recognises that Korea has established various avenues for the execution of individuals' rights of access, retention, deletion and suspension under PIPA. Those rights can be executed towards the controller itself or via a complaint lodged with the PIPC or other supervisory bodies, e.g. the National Human Rights Commission. Furthermore, the EDPB recognises the possibility to challenge controllers or public authorities' decision in response to their request on the basis of the Administrative Litigation Act.

185. In addition, The EDPB understands from the explanations given by the European Commission that individuals may challenge the actions of law enforcement and national security authorities before

competent courts under the Administrative Litigation Act and Constitutional Court Act, and have the possibility to obtain compensation for damages under the State Compensation Act[92].

186. In this context, however, the EDPB is concerned about effective redress for EU individuals in national security cases where no Korean citizen is involved. As noted in paragraph 33 et seq., national security authorities are not required to notify data subjects of the collection and processing of their personal data. Since it is considerably more difficult to obtain effective legal protection in these cases, the EDPB would like to point out that certain legal safeguards are required here if data transferred from the EEA is involved. These safeguards must enable data subjects to take effective action against unlawful data processing in a legally secure manner without being hindered by excessively narrow procedural requirements, e.g., by the imposition of a burden of proof that they cannot meet without knowledge of the processing. Furthermore, data subjects have to be able to turn to a competent body that meets the requirements of Article 47 CFR, i.e. which is competent to determine that a data processing is taking place, to verify the lawfulness of the processing, and to have enforceable remedial powers in the event the data processing is unlawful. Against this background, a mere right of complaint to the NHRC, for example, would not be sufficient. The EDPB therefore calls on the Commission to explain in more detail how these requirements are implemented in procedural and substantive terms, e.g., whether it is possible for data subjects to turn to the PIPC as well as to a court without having to prove the data processing in question.

187. In addition, the EDPB observes that the draft decision foresees a complaint referral mechanism, i.e. that EU individuals may submit a complaint to the PIPC through their national data protection authority or the EDPB. The PIPC will then notify the individual via the same channel once the investigation is concluded[93]. The EDPB welcomes the effort to facilitate easier access to redress against Korean national security authorities. At the same time, the EDPB advocates that such a referral mechanism is channelled through the European national data protection authorities rather than through the EDPB as they are competent and closer to the handling of the individual complaints.

188. Furthermore, the EDPB notes a possible contradiction with respect to voluntary disclosures. On the one hand, the draft decision states that individuals are able to obtain redress in case their data is disclosed unlawfully following a request for voluntary disclosure, including against the law enforcement authority issuing the request[94]. On the other hand, the draft decision makes reference to the requirement of direct impact regarding the individual's right to challenge the actions of public authorities, listing (only) binding disclosure requests as an example for a case where administrative action is considered to directly impact on the right to privacy[95]. The EDPB understands from explanations from the European Commission that there is actually no restriction of the redress possibilities against requests for voluntary disclosure and therefore asks the European Commission to further clarify this in the decision, both in the areas of law enforcement and national security (unlike the section on law enforcement, the section on voluntary disclosures for national security purposes does not contain any explicit statement on redress in this context).

[92] See Annex II, 3.2.4 in conjunction with 2.4.3.
[93] See Recital 205 and Annex I, p. 19 of the draft decision.
[94] See Recital 166 of the draft decision.
[95] See Recital 181(law enforcement) and Recitals 208 and 181 (national security) of the draft decision.