Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom

Adopted on 13 April 2021

CONTENTS

The European Data Protection Board

Having regard to Article 70(1)(s) of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the European Economic Area (hereinafter "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 endorsed its draft implementing decision (hereinafter "draft decision") on the adequate protection of personal data by the United Kingdom (hereinafter "UK") pursuant to the GDPR on 19 February 2021[2]. Following this, the European Commission initiated the procedure for its formal adoption.

2. On the same date, the European Commission asked for the opinion of the European Data Protection Board (hereinafter "EDPB")[3]. The EDPB's assessment of the adequacy of the level of protection afforded in the UK 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 by the European Commission.

3. The EDPB focused on the assessment of both the general GDPR aspects of the draft decision and on 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 UK legal framework are in place and effective.

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

[1] References to "Member States" made throughout this opinion should be understood as references to "EEA Member States".
[2] See European Commission's press release, Data protection: European Commission launches process on personal data flows to UK, 19 February 2021, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_661.
[3] Idem.
[4] See Article 29 Working Party, Adequacy Referential, adopted on 28 November 2017, as last revised and adopted on 6 February 2018, WP254 rev.01 (endorsed by the EDPB, see https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines); (hereinafter "*GDPR Adequacy Referential*").
[5] 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.

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 in the UK. It is important to recognise that the EDPB does not expect the UK legal 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. The UK data protection framework is largely based on the EU data protection framework (in particular the GDPR and Directive (EU) 2016/680 of the European Parliament and of the Council, hereinafter "EU Law Enforcement Directive" or "LED") which derives from the fact that the UK was a Member State of the EU up until 31 January 2020. Moreover, the UK Data Protection Act 2018, which came into force on 23 May 2018 and repealed the UK Data Protection Act 1998, further specifies the application of the GDPR in UK law, in addition to transposing the EU Law Enforcement Directive, as well as granting powers and imposing duties on the national data protection supervisory authority, the UK Information Commissioner's Office (hereinafter "ICO"). Therefore the EDPB recognises that the UK has mirrored, for the most part, the GDPR in its data protection framework.

7. **When analysing the law and practice of a third country which has been a Member State of the EU until recently, it is evident that the EDPB has identified many aspects to be essentially equivalent.**

8. In the area of data protection, the EDPB notes that there is a strong alignment between the GDPR framework and the UK legal framework on certain core provisions such as, for example, concepts (e.g., "personal data"; "processing of personal data"; "data controller"); grounds for lawful and fair processing for legitimate purposes; purpose limitation; data quality and proportionality; data retention, security and confidentiality; transparency; special categories of data; direct marketing; automated decision making and profiling.

1.2. Challenges

9. The United Kingdom was until recently a Member State of the EU; therefore, when analysing its law and practice, the EDPB has identified many aspects to be essentially equivalent. At the same time, in view of its role in the process of adopting an adequacy finding but also the time constraints, the EDPB has decided to focus its attention to those aspects where it considers that there is a need for closer look and more detailed scrutiny.

10. Nonetheless, challenges remain and the EDPB considers the following items should be further assessed to ensure that the essentially equivalent level of protection is met, and should be closely monitored in the UK by the European Commission.

1.2.1. General

11. The first challenge, a general one, relates to the monitoring of the evolution of the UK legal system on data protection as a whole. Indeed, the UK Government has indicated its intention to develop separate and independent policies in data protection with a possible will to diverge from EU data protection law. Such political declarations have not materialised yet in the UK legal framework. However, this possible future **divergence might create risks for the maintenance of the level of protection provided to personal data transferred from the EU. Therefore, the European Commission is invited to closely monitor such evolutions from the entry into force of its adequacy**

decision and take necessary actions including by amending and/or suspending the decision if necessary.

1.2.2. General data protection aspects

12. First, the so-called '**immigration exemption**', laid down under **Schedule 2 to the Data Protection Act 2018, Part 1**, paragraph 4, **is 'broadly' formulated**. In particular, it also applies in case personal data are not collected for the purpose of immigration control by a controller, but are made available by the latter to another controller who processes such personal data for the purpose of immigration control.

13. The EDPB invites the European Commission to verify the state of play of the proceedings *Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin)* and, since this judgment is not final (*res judicata*), to verify whether it is confirmed or reviewed by the appeal judgment, taking any update in this regard into account, and specifying it in the decision. **The EDPB calls also on the European Commission to provide in the adequacy decision further information on the immigration exemption[6], in particular in relation to the necessity and proportionality of such broad exemption in UK law, notably having regard to the broad scope of application *ratione personae*.** At the same time, the EDPB invites the European Commission to further explore whether additional safeguards exist in the UK legal framework or could be envisaged, for instance through legally binding instruments that would complement the immigration exemption by enhancing its foreseeability and the safeguards for the data subjects, also allowing for a better and prompt assessment and monitoring of the necessity and proportionality requirements.

14. Second, although the EDPB recognises that the UK has mirrored, for the most part, Chapter V GDPR in its data protection framework, the EDPB has identified certain aspects of the UK legal framework **with regard to onward transfers** that might undermine the level of protection of personal data transferred from the EEA.

15. Indeed, Article 44 GDPR[7] provides that transfers and onward transfers of personal data shall only take place if the level of protection of natural persons guaranteed by the GDPR is not undermined. **This means that not only the UK legislation shall be "essentially equivalent" to the EU legislation with regard to the processing of personal data transferred to the UK under the future adequacy decision, but also that the rules applicable in the UK with regard to the onward transfer of those data to third countries shall ensure that an essentially equivalent level of protection will continue to be provided.**

---

[6] Also as outcome of the ongoing review of the use of the immigration exemption referred to at p. 5 of the UK Government's Explanatory Framework for Adequacy Discussions, Section E3: Schedule 2 Restrictions, 13 March 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf.

[7] "*Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the Controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.*"

16. Although the EDPB notes the capacity of the UK, under its legal framework, to recognise territories as providing an adequate level of data protection in light of the UK data protection framework, the EDPB wishes to highlight that these territories might not benefit, to date, from an adequacy decision issued by the European Commission and ensure a level of protection "essentially equivalent" to that guaranteed in the EEA. This might lead to possible risks in the protection provided to personal data transferred from the EEA especially if, in the future, the UK data protection framework deviates from the EU acquis. In addition, the UK has already recognised as adequate the third countries that enjoy an adequacy finding by the European Commission under Directive 95/46/EC[8], while the European Commission will soon review these findings, and the conclusions of this review are not yet known.

17. **For the above situations, the European Commission should fulfil its monitoring role, and in case the essentially equivalent level of protection of personal data transferred from the EEA is not maintained, the European Commission should consider amending the adequacy decision to introduce specific safeguards for data transferred from the EEA and/or to suspend the adequacy decision.**

18. **Regarding international agreements concluded between the UK and third countries,** the European Commission is invited to examine the interplay between the UK data protection framework and its international commitments, beyond the Agreement on access to electronic data for the purpose of countering serious crime concluded between UK and the United States of America (hereinafter "US")[9] (hereinafter "UK-US CLOUD Act Agreement"), in particular to ensure the continuity of the level of protection where personal data are transferred from the EU to the UK on the basis of the UK adequacy decision, and then onward transferred to other third countries; and to continuously monitor and take action, where necessary, in the event that the conclusion of international agreements between the UK and third countries risks to undermine the level of protection of personal data provided for in the EU.

19. Furthermore, the European Commission is invited to monitor whether the UK-US CLOUD Act Agreement ensures appropriate additional safeguards, taking into account the level of sensitivity of the categories of data concerned and the sole requirements of the transfer of electronic evidence directly by service providers rather than between authorities, also assessing under which circumstances safeguards may be provided by an appropriate implementation of the adaptation of the EU-US Umbrella Agreement[10].

20. Further, the EDPB notes that onward transfers can also take place from the UK to another third country based on **transfer tools pursuant to the UK applicable data protection legislation[11]**. Following *Schrems II*[12], the EDPB invites the European Commission to provide reassurances in the

[8] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).
[9] See Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, Washington DC, USA, 3 October 2019, https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019.
[10] See Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences, December 2016 (hereinafter "EU-US Umbrella Agreement"), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3A3104_8.
[11] See Articles 46 and 47 UK GDPR.
[12] See *Schrems II*.

adequacy decision that necessary safeguards will be effectively put in place taking also into account the legislation of the receiving third country.

21. Concerning the absence **of protections provided under Article 48 GDPR** in the UK legislation, the EDPB invites the European Commission to provide further assurances and specific references to the UK legislation that ensure that the level of protection under the UK legal framework is essentially equivalent to the level of protection guaranteed in the EEA.

22. With regard to **procedural and enforcement mechanisms,** the EDPB notes that 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 are key elements a data protection framework consistent with the European one must be characterized by.

23. The EDPB acknowledges that the UK has mirrored in most parts the relevant provisions of the GDPR in the UK GDPR and in the Data Protection Act 2018; nevertheless, the European Commission is invited to continuously monitor any developments in the UK legal framework and practice, which might lead to detrimental impacts on those areas.

1.2.3. On the access by public authorities to data transferred to the UK

24. The EDPB notes the significant changes in the UK legal framework applicable to security and intelligence agencies, especially regarding the interception and acquisition of communication data. The EDPB understands that these changes are, *inter alia*, a response to the proceedings initiated before the CJEU and the European Court on Human Rights (hereinafter "ECtHR") and their recent judgments in this context.

25. In particular, the EDPB welcomes the fact that the UK has established the Investigatory Powers Tribunal (hereinafter "IPT"). The IPT is not only competent to hear cases on the use of investigatory powers by law enforcement authorities, but also by intelligence services. It is therefore the understanding of the EDPB that the IPT functions as a proper court in the meaning of Article 47 Charter of Fundamental Rights of the European Union (hereinafter "EU Charter").

26. Furthermore, the EDPB positively notes the introduction of "Judicial Commissioners" in the Investigatory Powers Act 2016 (hereinafter "IPA 2016") as a significant improvement. It understands that an important function of the Judicial Commissioners is to approve *ex ante* in individual cases different surveillance measures, including targeted interception and bulk acquisition of communication data (so-called "double lock" procedure).

27. However, in order to assess the effectiveness of this additional level of oversight, the EDPB sees the need to further clarification of the scenarios for which a lawful interception without approval by the Investigatory Powers Commissioner (hereinafter "IPC") or the Judicial Commissioners is possible, and invites the European Commission to further assess and demonstrate that, even in cases where the double-lock procedure does not apply, the UK legal framework provides for appropriate safeguards, including through effective *ex post* oversight and redress possibilities offered to individuals, thus ensuring a level of protection which is essentially equivalent to the one provided within the EU.

28. Furthermore, the EDPB invites the European Commission to further assess the conditions under which urgency can be invoked, and provide clarifications concerning the possible avenues for the exercise of rights for the data subjects concerned and possible redress avenues offered to them in

the context of equipment interference operations, especially in the case of a derogation to the double-lock procedure.

29. In addition, the EDPB considers that there is a need for further clarification and assessment of bulk interceptions, in particular on the selection and application of the selectors, in order to clarify the extent to which access to personal data meets the threshold set by the CJEU, and which safeguards are in place to protect the fundamental rights of individuals whose data are intercepted in this context, including concerning the retention periods of data. An independent assessment from competent UK oversight authorities would be particularly useful. The EDPB also underlines that it seems all the more critical that "overseas-related communications" which are within the scope of bulk interception practices appear to imply that data could be directly intercepted and collected in bulk within the EU by the UK, including for data in transit between the EU and the UK, which would fall within the scope of the draft decision. Given the importance of this aspect, the EDPB calls on the European Commission to closely monitor developments in this regard.

30. Still in relation to bulk interception, the EDPB stresses the consistent assessment by the ECtHR and the CJEU, and recalls the concerns expressed in relation to secondary data, which should benefit from specific safeguards due to their sensitivity. The EDPB therefore calls on the European Commission to carefully assess whether the safeguards provided under UK law for such category of personal data ensure an essentially equivalent level of protection to the one guaranteed in the EEA.

31. In this context, the EDPB is aware of the fact that the 2016 Intelligence and Security Committee's public report concerning the use of bulk powers[13] concerns practices under the previous legal framework, which was subsequently replaced by the IPA 2016. Nevertheless, it sees a need for further independent assessment and oversight of the use of automated processing tools by the competent UK oversight authorities, and calls on the European Commission to further assess this issue and the safeguards that would and/or could be afforded to EEA data subjects in this context.

32. The EDPB shares the view expressed by the IPC that further review and monitoring are needed to ensure that the safeguards, applied in practice by competent authorities in the field of national security and intelligence to remedy incompliances with the application of the relevant legislation, are maintained and will continue to be improved. The EDPB also welcomes the fact that consequently, the IPC conducted a review of its approach to inspecting bulk interception in 2019, "*which included a careful review of the technically complex ways in which bulk interception is actually implemented*" and committed to include "*a detailed examination of the selectors and search criteria alluded to above by the ECtHR*" in the inspections of bulk interception from 2020 onwards. Given the importance of this aspect, the EDPB is concerned that detailed examination of the selectors and search criteria has not been carried out yet by the IPC, and calls on the European Commission to closely monitor developments in this regard, especially since the concrete format of such oversight remains to be clarified.

33. The EDPB underlines that, when it comes to overseas disclosures, the application of national security exemption provided under UK law may lead to the absence of safeguards ensuring that the principles of purpose limitation, necessity and proportionality would also be respected or foreseeing that sufficient rights of the individuals, oversight and redress would also be provided or respected in the third country of destination. The EDPB therefore recommends the European Commission to further

[13] See Report of the bulk powers review, by the Independent Reviewer of Terrorism Legislation, August 2016, https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf.

examine the overall safeguards provided under UK law when it comes to overseas disclosure, in particular in light of the application of national security exemptions.

34. Finally, the EDPB is concerned about other forms of information sharing and disclosures, on the basis of other instruments, in particular the various international agreements concluded by the UK with other third countries, especially where these instruments remain inaccessible to the public, such as the UK-US Communication Intelligence Agreement. The effect of such agreement could lead to a circumvention of the safeguards identified in relation to the access and use of personal data for national security purposes. The EDPB considers that the conclusion of bilateral or multilateral agreements with third countries for the purpose of intelligence cooperation, providing a legal basis for direct interception and acquisition of personal data or the transfer of personal data to these countries may also significantly affect the conditions for further use of the information collected, since such agreements are likely to affect the UK data protection legal framework as assessed.

1.3. Conclusion

35. The EDPB considers that the UK adequacy assessment is unique because of the previous status of the UK as an EU Member State. Besides, it would also be the first adequacy decision including a sunset clause.

36. Accordingly, the EDPB recognises many areas of convergence between the UK and the EU data protection frameworks. At the same time, however, and following a careful analysis of the European Commission's draft decision and the UK data protection legislation, the EDPB has identified a number of challenges, which are examined extensively in this opinion. In this context, the EDPB wishes to emphasise the paramount role of the European Commission on the monitoring of all relevant developments in the UK.

37. In light of the above, the EDPB recommends the European Commission to address the challenges raised in this opinion. The EDPB also invites the European Commission to monitor closely all relevant developments in the UK that may have an impact on the essential equivalence of the level of protection of personal data, and to take swiftly appropriate actions, where necessary.

2. INTRODUCTION

2.1. UK data protection framework

38. The UK data protection framework is largely based on the EU data protection framework (in particular the GDPR and the LED), which derives from the fact that the UK was a Member State of the EU up until 31 January 2020. Moreover, the UK Data Protection Act 2018, which came into force on 23 May 2018 and repealed the UK Data Protection Act 1998, further specifies the application of the GDPR in UK law, in addition to transposing the EU Law Enforcement Directive, as well as granting powers and imposing duties on the national data protection supervisory authority, the UK ICO.

39. As mentioned in recital 12 of the European Commission's draft decision, the UK Government enacted the European Union (Withdrawal) Act 2018, which incorporates directly applicable EU legislation into the law of the UK. Under this Act, the ministers of the UK have the power to introduce secondary legislation, via statutory instruments, to make the necessary modifications to retained EU law following the UK's withdrawal from the EU to fit the domestic context.

40. Consequently, the relevant legal framework applicable in the UK after the end of the transition period[14] consists of:

- the United Kingdom General Data Protection Regulation (hereinafter "UK GDPR"), as incorporated into the law of the UK under the European Union (Withdrawal) Act 2018, as amended by the DPPEC (Data Protection, Privacy and Electronic Communications (Amendment Etc.) (EU Exit)) Regulations 2019;
- the Data Protection Act 2018 (hereinafter "DPA 2018"), as amended by the DPPEC Regulations 2019, and the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020; and
- the IPA 2016.

(together "the UK Data Protection Framework").

2.2. Scope of the EDPB's assessment

41. The draft decision of the European Commission is the result of an assessment of the UK Data Protection Framework, followed by discussions with the UK 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.

42. As mentioned in the GDPR Adequacy Referential: "*the information provided by the European Commission should be exhaustive and put the EDPB in a position to make an own assessment regarding the level of data protection in the third country*"[15].

43. In this regard, it is to be noted that the EDPB only partially received documents relevant for the examination of the UK legal framework on time. The EDPB received most part of the UK legislation referred to in the draft decision through links referenced in the latter. The European Commission was not in a position to provide the EDPB with written explanations and commitments from the UK in relation to the exchanges between the UK authorities and the European Commission relevant to this exercise[16].

[14] The transition period is set for 31 December 2020, after which date EU law no longer applies in the UK. The "bridge period" is set for 30 June 2021 at the latest, and refers to the additional period during which transmission of personal data from the EEA to the UK is not deemed a transfer.

[15] See WP254 rev.01, p. 3.

[16] With regard to: Article 48 GDPR (footnote 78 of the draft decision); enhanced safeguards and security measures applied by controllers when processing in the national security context (footnote 64 of the draft decision); to the requirement for the controller to consider whether there is a need to rely on the exemption on a case-by-case basis even where a national security certificate has been issued (recital 126 and footnote 172 of the draft decision); the fact that the protections of the EU-US Umbrella Agreement will apply to all personal information produced or preserved under the UK-US CLOUD Act Agreement, irrespective of the nature or type of body making the request, with regard to the details of the concrete implementation of the data protection safeguards which are still subject to discussions between the UK and the US, the confirmation that UK authorities will only let this Agreement enter into force once they are satisfied that its implementation complies with the legal obligations provided therein, including clarity with respect to compliance with the data protection standards for any data requested under this Agreement (recital 153 of the draft decision); situations where data are transferred from the EU to the UK within the scope of this draft decision, and the fact that there would always be a "British Islands connection" and any equipment interference covering such data would

44. Taking into account the above, and due to the limited timeframe (2 months) afforded to the EDPB to adopt this opinion, the EDPB has chosen to focus on some specific points presented in the draft decision and provide its analysis and opinion on them.

45. When analysing the law and practice of a third country which has been a Member State of the EU until recently, it is evident that the EDPB has identified many aspects to be essentially equivalent. In view of its role in the process of adopting an adequacy finding and the amount of law and practice to be analysed, the EDPB has decided to focus its attention to those aspects where it saw the greatest need to look closer. 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 UK, and the practice of the national security apparatus in the UK. However, it has to be borne in mind that national security is evidently an area of law and practice where the legislation of Member States is not harmonised at EU level and therefore may differ.

46. The EDPB took into account the applicable European data protection framework, including Articles 7, 8 and 47 EU 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 of the European Convention on Human Rights (hereinafter "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.

47. 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 UK. The concept of "adequate level of protection", which already existed under Directive 95/46/EC, 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*"[17]. 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 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 of such rules. Efficient enforcement mechanisms are of paramount importance to the effectiveness of data protection rules[18].

2.3. General comments and concerns

therefore be subject to the mandatory warrant requirement of section 13(1) of the IPA 2016 (recital 206 of the draft decision); and the examples of operational purposes provided (recital 216 and footnote 369 of the draft decision).

[17] See CJEU, C-362/14, *Maximilian Schrems v Data Protection Commissioner*, 6 October 2015, ECLI:EU:C:2015:650 (hereinafter "*Schrems I*"), paras. 73-74.

[18] See WP254 rev.01, p.2.

2.3.1. International commitments entered into by the UK

48. According to Article 45(2)(c) GDPR and the GDPR Adequacy Referential[19], 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. Furthermore, the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data (hereinafter "Convention 108"),[20] and its Additional Protocol[21], should be taken into account.

49. **In this regard, the EDPB welcomes that the UK has adhered to the ECHR and is under the jurisdiction of the ECtHR. In addition, the UK has also adhered to Convention 108 and its Additional Protocol, has signed Convention 108+[22] in 2018, and is currently working on its ratification.**

2.3.2. Possible future divergence of the UK Data Protection Framework

50. As mentioned in recital 281 of the draft decision, the European Commission must take into account that, with the end of the transition period provided by the Withdrawal Agreement[23], the UK administers, applies and enforces its own data protection regime, and as soon as the bridge provision under Article FINPROV.10A of the EU-UK Trade and Cooperation Agreement[24] ceases to apply, this may notably involve amendments or changes to the data protection framework assessed in the draft decision, as well as other relevant developments.

51. The European Commission has therefore decided to include a sunset clause in its draft decision[25], setting the expiration date of four years after its entry into force.

52. It is important to note that the possibility of the UK ministers and the UK Secretary of State to introduce secondary legislation following the end of the bridge period may lead to a significant divergence of the UK Data Protection Framework from the EU's in the future.

53. Indeed, the UK Government has indicated its intention to develop separate and independent policies in data protection, which may then lead to a divergence from EU data protection law[26]. This intention

---

[19] See WP254 rev.01, p.2.

[20] See Convention for the protection of individuals with regard to the processing of personal data, Convention 108, 28 January 1981.

[21] See Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, opened for signature on 8 November 2001.

[22] See Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108+"), 18 May 2018.

[23] See Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community (OJ L 029, 31.1.2020, p. 7).

[24] See Trade and cooperation agreement between the European union and the European atomic energy community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part (OJ L 444, 31.12.2020, p. 14).

[25] See Article 4 of the draft decision. See also recital 282 of the draft decision.

[26] The UK's National Data Strategy (last updated on 9 December 2020, https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy) includes the following as one of its missions: "*Championing the international flow of data. The flow of information across borders fuels global business operations, supply chains and trade, powering growth across the world. It also plays a wider societal role. The transfer of personal data ensures people's salaries are paid, and helps them connect with loved ones from afar. And, as the coronavirus pandemic has demonstrated, sharing health data*

encompasses the inclusion of personal data aspects in trade agreements[27], a practice that entails the risk of lowering the level of protection of personal data provided for by the UK[28].

54. Finally, not only since the end of the transition period, the UK is no longer bound by CJEU case-law but also, the already adopted judgments of the CJEU, considered as retained case law in the UK legal framework, might not bind the UK any more as, in particular, the UK has the possibility to modify retained EU law after the end of the bridge period and its Supreme Court is not bound by any retained EU case-law[29].

55. **Considering the risks related to the possible deviation of the UK Data Protection Framework from the EU acquis following the end of the bridge period, the EDPB welcomes the European Commission's decision to introduce a sunset clause of four years for the draft decision. However, the EDPB would like to highlight here the importance of the European Commission's monitoring role[30]. Indeed, the European Commission should monitor all relevant developments in the UK that may have an impact on the essential equivalence of the level of protection of personal data transferred under the UK adequacy decision on an ongoing and permanent basis from its entry into force. In addition, the European Commission should take appropriate action by suspending, amending or repealing the adequacy decision, based on the circumstances at hand, if after the adequacy decision is adopted, the European Commission has indications that an adequate level of protection is no longer ensured in the UK.**

56. On its side, the EDPB will use its best efforts to inform the European Commission about any relevant action undertaken by Member State's data protection supervisory authorities (hereinafter "SAs") either in the commercial or public sector, and in particular regarding complaints made by data subjects in the EEA concerning the transfer of personal data from the EEA to the UK.

---

can aid vital scientific research into diseases while uniting countries in their response to global health emergencies. ***Having left the European Union, the UK will champion the benefits that data can deliver.*** *We will promote domestic best practice and work with international partners* ***to ensure data is not inappropriately constrained by national borders and fragmented regulatory regimes*** *so that it can be used to its full potential*." (emphasis added).

[27] Ibid: "*Facilitate cross-border data flows:* ***We will work globally to remove unnecessary barriers to international data flows. We will agree ambitious data provisions in our trade negotiations*** *and use our newly independent seat in the World Trade Organisation to influence trade rules for data for the better.* ***We will remove obstacles to international data transfers*** *which support growth and innovation, including by developing a new UK capability that delivers new and innovative mechanisms for international data transfers. We will also work with partners in the G20 to create interoperability between national data regimes to minimise friction when transferring data between different countries"*. (emphasis added).

[28] See European Parliament resolution of 12 December 2017 "*Towards a digital trade strategy*" (2017/2065(INI)), Section V, in which it stressed that "*The protection of personal data is non-negotiable in [EU] trade agreements*", available at: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0488_EN.pdf. See also, European Parliament resolution of 25 March 2021 on the Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application, para. 28 in which it is stated: *"supports the Commission's practice of addressing data protection and personal data flows separately from trade agreements"*, https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_EN.html.

[29] See section 6(3) to (6) EU (Withdrawal) Act 2018.

[30] See Article 45(4) GDPR.

3. GENERAL DATA PROTECTION ASPECTS

3.1. Content principles

57. Chapter 3 of the GDPR Adequacy Referential is dedicated to the "Content Principles". A third country's system must contain them in order for its level of data protection to be considered essentially equivalent to the one guaranteed within the EU. The EDPB acknowledges the fact that the UK does not have a codified constitution in that there is no one single document that sets out its governing fundamental rules. However, the right to respect for private and family life (and the right to data protection as part of that right) and the right to a fair trial[31] are included in the Human Rights Act 1998, and the constitutional value of this statute has been recognised by UK courts. Indeed, the Human Rights Act 1998 incorporates the rights contained in the ECHR[32]. In addition, the Human Rights Act 1998 states very importantly that any action of public authorities must be compatible with the ECHR[33].

58. Aside from structural and formalistic differences between the UK and EU legislation, the EDPB notes, as one can expect, that the UK's approach to data protection is similar to the one in the EU resulting from the fact that the UK was a Member State of the EU up until 31 January 2020. As a result, many content principles are aligned with the GDPR's; therefore provide a level of protection essentially equivalent to the one provided by the EU. The EDPB has decided not to develop further the analysis as to those content principles that are in alignment with EU legislation, and is satisfied with the analysis provided by the European Commission in its draft decision. Such content principles are for example the following: concepts (e.g., "personal data"; "processing of personal data"; "data controller"); grounds for lawful and fair processing for legitimate purposes; purpose limitation; data quality and proportionality; data retention, security and confidentiality; transparency; special categories of data; direct marketing; automated decision making and profiling. The EDPB further notes that the UK GDPR and the DPA 2018 include content principles that go further than what is required by the GDPR Adequacy Referential and mirror the principles included in the GDPR; therefore elevating the level of protection provided for in the UK. Such content principles are for example the ones related to personal data breach notifications, the data protection officer, data protection impact assessments and data protection by design and by default.

59. However, as mentioned in the Introduction, the EDPB wishes to specifically address in this opinion certain points on which the EDPB has concerns and would like to request clarifications from the European Commission.

3.1.1. Rights of access, rectification, erasure and objection

60. The so-called 'immigration exemption', laid down under **Schedule 2 to the DPA 2018, Part 1**, paragraph 4 allows controllers involved in "immigration control" to not apply certain data subjects' rights provided by the DPA 2018 if this would be likely to "*prejudice the maintenance of effective immigration control*" or "*the investigation or detection of activities that would undermine the maintenance of effective immigration control*".

[31] See Articles 6 and 8 ECHR (Schedule 1 to the Human Rights Act 1998).
[32] For more information, see recitals 8-10 of the draft decision.
[33] See section 6 Human Rights Act 1998.

61. As acknowledged by the European Commission in its draft decision[34], and referred to in the Opinion of the LIBE Committee of the European Parliament, on the conclusion, on behalf of the EU, of the Trade and Cooperation Agreement between the EU and the UK[35], this exemption is **'broadly' formulated**. It applies to the following rights: right to be informed; right of access; right to erasure; right to restrict processing; and right to object.

62. Besides, it is important to note that this exemption also applies in case personal data are not collected for the purpose of immigration control by a controller ("controller 1"), but are however made available by the latter to another controller ("controller 2") who processes such personal data for the purpose of immigration control (e.g., the UK Home Office)[36].

63. In *Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin) (03 October 2019)*, the applicants challenged the lawfulness of the immigration exemption on the ground that it was contrary to Article 23 GDPR and incompatible with the rights guaranteed by Articles 7 and 8 EU Charter relating to privacy and the protection of personal data. The High Court of England and Wales (hereinafter "High Court") considered whether the immigration exemption in paragraph 4 of Part 1 of Schedule 2 of the DPA 2018 is lawful, and concluded in favour of its lawfulness.

64. The High Court considered in particular that:

---

[34] See recitals 62-65 of the draft decision.

[35] In this regard, on the **broad formulation** of the immigration exemption, see Opinion of the Committee on Civil Liberties, Justice and Home Affairs on the conclusion, on behalf of the Union, of the Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part and the United Kingdom of Great Britain and Northern Ireland, of the other part, and of the Agreement between the European Union and United Kingdom of Great Britain and Northern Ireland concerning security procedures for exchanging and protecting classified information (2020/0382(NLE)), 5 February 2021, https://www.europarl.europa.eu/doceo/document/LIBE-AL-680848_EN.pdf, para. 10: *"recalls, in this regard, Parliament's February and June 2020 resolutions, pointing out the **general and broad exemption** for the processing of personal data for immigration purposes of the UK Data Protection Act"*, and para. 11: *"considers that the **general and broad** exemption for the processing of personal data for immigration purposes of the UK Data Protection Act [...] need to be amended before a valid adequacy decision can be granted;"*(emphasis added).

[36] See example provided in the ICO "Guide to the General Data Protection Regulation (GDPR)", v 01 January 2021, p. 307 (emphasis added): *"A private organisation (controller 1) alerts the Home Office (controller 2) to an employee who is believed to have submitted false documents to evidence their identity and qualifications to obtain a job. The employer provides the Home Office with the relevant information. The right of the individual to be informed that their personal data has been passed to the Home Office is restricted in so far as giving effect to it would be likely to prejudice the investigation.*
*The **employer is therefore under no obligation to inform the individual that their information has been passed to the Home Office**, and in turn **the Home Office** is under no obligation to provide the individual with a privacy notice informing them that it is now processing their personal data. The exemption applies to both controllers to the same extent.*
*However, the employee requests a copy of their personal data from the Home Office which is now investigating them. The **Home Office may rely on the exemption** to withhold part of their data if the disclosure would be likely to prejudice the investigation. Should the employee make a similar request to **their employer, they would also be able to apply the exemption** to the same extent."*
In other words, as clarified on p. 300: *"In the majority of cases the Home Office, or one of its agencies and contractors, will be the controller applying this exemption. However, it is important to note that the application of this exemption is not just limited to the Home Office. It may also be relevant to other controllers such as employers, universities and the police, who liaise with the Home Office on immigration matters."*

- *"[…] the Immigration Exemption is plainly a matter of "important public interest" and pursues a legitimate aim.[…]"*, para. 30;
- *"the Immigration Exemption satisfies the requirements for a measure to be "in accordance with the law. […]"*, para. 38;
- *"The Immigration Exemption may only be relied on if and to the extent that compliance with "the listed GDPR provisions"* ***would be likely to prejudice*** *the maintenance of effective immigration control or the investigation or detection of activities that would undermine the maintenance of effective immigration control. The words "would be likely to prejudice", in the context of the Data Protection Act 1998 (which preceded the DPA 2018), were interpreted to mean "a very significant and weighty chance of prejudice to the particular public interest. The degree of risk must be such that there 'may very well' be prejudice to those interests, even if the risk falls far short of being more probable than not […]."*, para. 39 (emphasis added).

65. It should be noted that this judgment is, to the EDPB's knowledge, not final and has been appealed.

66. As specified in the EDPB Guidelines on restrictions under Article 23 GDPR ("the Article 23 GDPR Guidelines")[37] *"[...] in a GDPR context, restrictions shall be* ***provided for in a legislative measure****, concern a* ***limited number of rights of data subjects and/or controller's obligations*** *which are listed in Article 23 of the GDPR,* ***respect the essence*** *of the fundamental rights and freedoms at issue, be a* ***necessary and proportionate measure*** *in a democratic society and safeguard one of the grounds set out in Article 23(1) of the GDPR [...]"*.[38]

67. The EDPB also recalls that recital 41 GDPR states that *"[w]here this Regulation refers to* ***a legal basis or a legislative measure****, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a legal basis or legislative measure should be* ***clear and precise and its application should be foreseeable to persons subject to it****, in accordance with the case-law of the Court of Justice of the European Union [...] and the European Court of Human Rights"* (emphasis added).

68. Although the ECtHR specified that "*[f]urther, as regards the words "in accordance with the law" and "prescribed by law" which appear in Articles 8 to 11 of the Convention, the [ECHR] observes that it has always understood the term "law" in its "substantive" sense, not its "formal" one; it has included both "written law", encompassing enactments of lower ranking statutes and regulatory measures taken by professional regulatory bodies under independent rule-making powers delegated to them by Parliament, and unwritten law. "Law" must be understood to include both statutory law* ***and judge-made "law""***[39], the Article 23 GDPR Guidelines recall that *"[a]ccording to the CJEU case law, any* ***legislative measure*** *adopted on the basis of Article 23(1) [of the] GDPR must, in particular,* ***comply with the specific requirements set out in Article 23(2) of the GDPR****. Article 23(2) [of the] GDPR states that the legislative measures imposing restrictions to the rights of data subjects and the controllers' obligations shall contain, where relevant,* ***specific provisions about several criteria***

[37] See EDPB Guidelines 10/2020 on restrictions under Article 23 GDPR, version 1.0, adopted on 15 December 2020, which are currently under finalisation following public consultation, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-102020-restrictions-under-article-23_en.

[38] See Article 23 GDPR Guidelines, para. 9, p. 5.

[39] See ECtHR, *Sanoma Uitgevers B.V. v. The Netherlands*, 14 September 2010, EC:ECHR:2010:0914JUD003822403, para. 83 (emphasis added).

***outlined below**. As a rule, all the requirements detailed below **should be included in the legislative measure** imposing restrictions under Article 23 [of the] GDPR."*[40]

69. It can be observed in this regard that **the immigration exemption** itself **does not specify the following elements referred to under Article 23(2) GDPR**:

- "the safeguards to prevent abuse or the unlawful access or transfer" (d);
- "the controller or categories of controllers" (e)[41];
- "the risks to the rights and freedoms of data subjects" (g);
- "the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction" (h).

70. The ICO's "Guide to the General Data Protection Regulation (GDPR)"[42], including a Chapter on the "immigration exemption", does provide clarifications on the immigration exemption, but **cannot** *per se* provide binding rules complementing it. Moreover, the issue of 'quality of the law' is particularly relevant given the importance of the restricted rights and the extension of the exemption[43].

---

[40] See Article 23 GDPR Guidelines, paras. 45 and 46, p. 11. Under Article 52(3) EU Charter, *"[i]n so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection"*. On the notion of '**provided for by law**' under Article 52(1) EU Charter, the criteria developed by the ECtHR should be used as suggested in several CJEU Advocate General's Opinions, see for example the Opinions in joined cases C-203/15 and C-698/15, *Tele2 Sverige AB*, ECLI:EU:C:2016:572, paras. 137-154, and in case C-70/10, *Scarlet Extended*, ECLI:EU:C:2011:255, paras. 88-114. Hence, reference can be made, among others, to the ECtHR ruling in *Weber and Saravia v Germany*, para. 84: *"The Court reiterates that the expression "**in accordance with the law**" within the meaning of Article 8 § 2 [of the ECHR] requires, firstly, that the impugned measure should have some basis in **domestic law**; it also refers to the **quality of the law** in question, requiring that it should be accessible to the person concerned, who must, moreover, be able to foresee its consequences for him, and compatible with the rule of law."*(emphasis added).
See also recital 41 GDPR: *"Such [a legal basis or] legislative measure should be **clear** and **precise** and its application should be **foreseeable to persons subject** to it, in accordance with the case-law of the Court of Justice of the European Union (...) and the European Court of Human Rights"* (emphasis supplied).

[41] See the aforementioned High Court case, para. 54: *"In my view there is nothing unlawful about the Immigration Exemption being available **to all data controllers** processing data for the specified purposes. As the defendants point out, without paras 4(3)–(4) the Immigration Exemption would be rendered ineffective in cases where data is obtained from third parties (such as a local authority or HM Revenue and Customs) for the purposes of maintaining effective immigration control."* (emphasis added), hence confirming the **generalised** application of the restrictions.

[42] ICO's "Guide to the General Data Protection Regulation (GDPR)", v 01 January 2021, p. 299-307.

[43] See para. 57 of the aforesaid High Court case: *"Mr Knight informs me that the Commissioner is finalising guidance on the Exemption, but it will have "statutory" status only in the sense of being issued by virtue of the Commissioner's powers under art.57(1) of the GDPR. It will have no legal status under DPA 2018."*
The rationale for the introduction of legally binding guidance supported by ICO is referred to in particular at paras. 56-60 of the judgment:
"56. Finally, I turn to the Commissioner's submission that without accompanying statutory guidance to provide safeguards as to the meaning and application of the Immigration Exemption, the exemption would not be a proportionate implementation of art.23(1) of the GDPR. Mr Knight says that supplemented by such guidance, the provision is proportionate.
57. Mr Knight informs me that the Commissioner is finalising guidance on the Exemption, but it will have "statutory" status only in the sense of being issued by virtue of the Commissioner's powers under art.57(1) of

71. *A fortiori*, the "**prejudice test**" does not set out the safeguards to prevent abuse or unlawful access or transfer, and to be implemented for instance by the Home Office.

72. In the light of all of the above, the EDPB remarks that further clarifications on the application of the immigration exemption are needed.

73. Furthermore, the EDPB remarks the lack of a legally binding instrument that clarifies the immigration exemption in view of considering whether it is essentially equivalent with Article 23 GDPR and Articles 7 and 8 EU Charter. At the same time, the EDPB considers that the necessity and proportionality of the broad scope *ratione personae* of the immigration exemption needs to be further demonstrated by the European Commission, supported by evidence.

74. **As a conclusion, the EDPB invites the European Commission to verify the state of play of the proceedings *Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin)* referred to above and, since this judgment is not final (*res judicata*), to verify whether it is confirmed or reviewed by the appeal judgment, to take any update in this regard into account, and to specify it in the adequacy decision. The EDPB also calls on the European Commission to provide further information on the necessity and**

---

the GDPR. It will have no legal status under DPA 2018. I understand also that the Home Office has produced draft internal staff guidance on the Immigration Exemption (see [22] above). In practice guidance issued by the Commissioner is influential regardless of its legal basis. However, there is no power for the Commissioner to issue "binding" guidance of the sort that the Supreme Court had in mind in the Christian Institute case (at [101] and [107]). It appears that primary legislation would be required if it were considered necessary for there to be guidance on the Immigration Exemption of the same status as the codes of practice currently provided for in ss.121–124 of DPA 2018.

58. In his argument for statutory guidance Mr Knight contends that the context in which the use of the Immigration Exemption will arise necessarily frames the concerns about the necessity and proportionality of its existence and use. He draws attention to two matters in particular in the legal context. First, personal data to which the Immigration Exemption is applied is inherently likely to involve special category data within the meaning of art.9(1) of the GDPR (i.e. data "revealing racial or ethnic origin"). Such data is identified in the GDPR because it requires a higher measure of protection (Opinion 1/15 [2019] 3 C.M.L.R. 25 at [141]). Secondly, it is a basic proposition of data protection law that the right of subject access in particular is of great importance as the gateway to being able to exercise the other rights provided to data subjects (see YS v Minister voor Immigratie, Integratie en Asiel (C-141/12) EU:C:2014:2081; [2015] 1 C.M.L.R. 18 at [44]).

59. Mr Knight identifies four points of a practical nature. First, when controllers do not explain to data subjects that they have relied upon a statutory exemption, nor provide a broad summary of the reasons why, the data subject will be unaware that the exemption has been applied, and unable to challenge it effectively as a result. Secondly, data subjects will be especially reliant on controllers to apply the exemption with care and only so far as necessary. Although any data subject is entitled to complain to the Commissioner about the application of the exemption, or to bring legal proceedings before the courts, it is likely that the data subject will be unaware of their rights and lack the funds to take legal steps, in circumstances where there is a need for prompt and accurate compliance with data protection rights. Thirdly, as an immigrant the data subject is likely to be in a vulnerable position. Fourthly, this is not an abstract issue in the light of the defendants' evidence as to the use of the Immigration Exemption (see [4] above).

60. Mr Knight suggests that there is a close parallel between the present challenge to the Immigration Exemption and the reasoning of the Court in Christian Institute [2016] UKSC 51 . As in Christian Institute , he contends, the Immigration Exemption is wide, uses undefined terms, applies a low threshold, is subject to controls not apparent on the face of the provision and applies to a very broad array of contexts and rights. Unlike Christian Institute there is no publicly available guidance, still less of a statutory status even to which regard must be had, on the Immigration Exemption."

proportionality of the immigration exemption, in particular having regard to the broad scope of application *ratione personae*.

75. **At the same time, the EDPB invites the European Commission to further explore whether additional safeguards exist in the UK legal framework or could be envisaged, for instance through legally binding instruments that would complement the immigration exemption enhancing its foreseeability by and the safeguards for data subjects, also allowing for a better and prompt assessment and monitoring of the necessity and proportionality requirements.**

3.1.2. Restrictions on onward transfers

76. Article 44 GDPR provides that transfers and onward transfers of personal data shall only take place if the level of protection of natural persons guaranteed by the GDPR is not undermined. Therefore, personal data transferred from the EEA to the UK based on the adequacy decision shall enjoy an essentially equivalent level of protection to the one provided under the EU data protection framework. **This means that not only the UK legislation shall be "essentially equivalent" to the EU legislation with regard to the processing of personal data transferred to the UK under the draft decision, but also that the rules applicable in the UK with regard to the onward transfer of those data to third countries shall ensure that an essentially equivalent level of protection will continue to be provided.**

77. As a result, it is important that any onward transfer from the UK to another third country of personal data from the EEA is properly protected with safeguards, or is carried out in accordance with the rules on derogations[44] to ensure the continuity of protection afforded by the EU legislation. **Indeed, if no such protection can be provided, onward transfers of EEA personal data should not take place.**

78. The EDPB recognises that the UK has mirrored, for the most part, Chapter V GDPR in the UK GDPR (Articles 44-49) and in the DPA 2018[45]. **However, the EDPB has identified certain aspects of the UK legislative framework with regard to onward transfers that might undermine the level of protection of personal data transferred from the EEA.**

79. **The first challenge** the EDPB has identified relates to the recognition by the UK, following the procedure as elaborated in the DPA 2018, of third countries, international organisations or territories[46] as adequate recipients. Indeed, onward transfers of EEA personal data may occur from the UK to other third countries, on the basis of a future possible UK adequacy regulation[47].

80. More specifically, as explained in recital 77 of the draft decision, the UK Secretary of State has the power to recognise a third country (or a territory or a sector within a third country), an international organisation, or a description of such a country, territory, sector, or organisation as ensuring an adequate level of protection of personal data, following consultation of the ICO[48]. When assessing the adequacy of the level of protection, the UK Secretary of State must consider the same elements that the European Commission is required to assess under Article 45(2)(a)-(c) GDPR, interpreted together with recital 104 GDPR and the retained EU case-law. This means that, when assessing the

[44] See Article 49 UK GDPR.
[45] See section 17A, 17B, 17C and 18 DPA 2018.
[46] See section 17A of DPA 2018 DPA 2018.
[47] The UK equivalent to an adequacy decision under the GDPR.
[48] See section 182(2) DPA 2018. See also the Memorandum of Understanding on the role of the ICO in relation to new UK adequacy assessments, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/03/secretary-of-state-for-the-department-for-dcms-and-the-information-commissioner-sign-memorandum-of-understanding/.

adequate level of protection of a third country, the relevant standard will be whether that third country in question ensures a level of protection "essentially equivalent" to that guaranteed within the UK. Although the EDPB notes the capacity of the UK, under the UK GDPR, to recognise territories as providing an adequate level of protection in light of the UK Data Protection Framework, the EDPB wishes to highlight that these latter territories might not benefit, to date, from an adequacy decision issued by the European Commission recognising a level of protection "essentially equivalent" to that guaranteed in the EU. This might lead to possible risks in the protection provided to personal data transferred from the EEA, especially if the UK Data Protection Framework were to deviate from the EU acquis in the future. It is to be noted that in July 2020, the *Schrems II* CJEU landmark case[49] resulted in the invalidation of the US Privacy Shield Decision as, according to the CJEU, the US legal framework could not be considered as providing an essentially equivalent level of protection compared to the one of the EU. However, the already adopted judgments of the CJEU, considered as retained case-law in the UK legal framework, might not bind the UK anymore as, in particular, the UK has the possibility to modify retained EU law after the end of the bridge period, and its Supreme Court is not bound by any retained EU case law[50].

81. **The EDPB invites the European Commission to closely monitor the adequacy assessment process and criteria by UK authorities with regard to other third countries, in particular with respect to third countries not recognised as adequate under the GDPR by the EU. Where the European Commission finds that no essentially equivalent level of protection to that guaranteed within the EU is ensured by a third country found adequate by the UK, the EDPB invites the European Commission to take any and all necessary steps such as, for example, amending the UK adequacy decision to introduce specific safeguards for personal data originating from the EEA, and/or to consider the suspension of the UK adequacy decision, where personal data transferred from the EEA to the UK are subject to onward transfers to the third country in question on the basis of a UK adequacy regulation.**

82. **The second challenge** relates to the upcoming review of the already existing adequacy decisions rendered by the European Commission under Directive 95/46/EC. Following this review, the European Commission might decide that certain countries that benefited until now from an adequacy decision no longer provide for an essentially equivalent level of protection taking into account the current EU legislation and recent case-law. However, as provided for in paragraph 4, Schedule 21 DPA 2018, the UK has already recognised those countries as providing for an adequate level of protection. Even though the UK Secretary of State must conduct a review of these adequacy findings within a period of four years, the European Commission notes in its draft decision that these adequacy findings will not automatically cease to exist should the UK Secretary of State not undertake the required review within the stipulated four-year time limit[51].

83. **The EDPB invites the European Commission to monitor whether, once the EU review of the already existing adequacy decisions is finalised, a country, deemed to no longer provide for an adequate level of protection, is still considered as such by the UK. If this is the case, the EDPB invites the European Commission, based on recitals 277 – 280 of the draft decision to take any appropriate measures to remedy the situation, for example by amending the adequacy decision in order to add specific requirements for personal data originating from the EEA and/or by suspending the adequacy decision, if personal data transferred from the EEA to the UK are subject to onward**

[49] See *Schrems II*.
[50] See section 6(3) to (6) EU (Withdrawal) Act 2018.
[51] See recital 82 of the draft decision.

transfers to the third country in question. The EDPB invites the European Commission to continue this monitoring exercise for the duration of the UK adequacy decision.

84. **The third challenge** concerns the onward transfer of personal data from the EEA to non-adequate countries based on the transfer tools provided for in Articles 46 and 47 UK GDPR. Although the UK GDPR provides for the same transfer tools as the ones provided by the GDPR, the EDPB highlights the need to ensure that the safeguards they contain provide for an effective protection in the third country, especially in the light of the *Schrems II* judgment.

85. Following the *Schrems II* ruling, in which the CJEU reminds that the protection granted to personal data in the EU must travel with the data wherever it goes, the EDPB has already adopted initial recommendations on supplementary measures[52] to assist exporters, where required, in ensuring that data subjects are afforded a level of protection essentially equivalent to that guaranteed within the EU.

86. According to the CJEU, data exporters are responsible for verifying, on a case-by-case basis and, where appropriate, in collaboration with the data importer in the third country, if the law or practice of the third country impinges on the effectiveness of the appropriate safeguards contained in the Article 46 GDPR transfer tools[53]. Where this is the case, data exporters should implement supplementary measures that fill these gaps in the protection and bring it up to the level required by EU law.

87. **The EDPB invites the European Commission, in order to ensure continuity of protection, to introduce in the draft decision reassurances that when the transfer tools provided in Articles 46 and 47 UK GPDR are used by data exporters in the UK for onward transfers to other third countries of EEA transferred data, these data exporters assess on a case-by-case basis, the data protection framework of the third country; and if necessary, take appropriate measures to ensure the effective respect of the safeguards contained in the chosen transfer tool to ensure an essentially equivalent level of protection to that guaranteed within the EU. Without these reassurances, the EDPB stresses that that there is a risk that the essentially equivalent level of protection to the one guaranteed within the EU, will be watered down through onward transfers taking place from the UK.**

88. **The fourth challenge** relating to onward transfers concerns the international agreements concluded, or to be concluded in the future by the UK and the possible direct access, by authorities from third country(ies) party(ies) to such agreements, to personal data from the EEA. Indeed, the EDPB has strong concerns in relation to the already concluded UK-US CLOUD Act Agreement and the European Commission acknowledges this challenge, stressing that "*a possible entry into force of the Agreement may impact the level of protection assessed in this Decision*"[54]. Indeed, based on this agreement, once it enters into force, personal data transferred from the EEA to the UK under the draft decision would then be subject to the provisions of this agreement laying down conditions for direct access by US authorities, impacting the UK Data Protection Framework, including the provisions on onward transfers. As a result, the level of protection provided to the data transferred from the EEA may be

[52] See EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, adopted on 10 November 2020, which are currently under finalisation following public consultation, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf.

[53] See *Schrems II*, para. 134.

[54] See recital 153 of the draft decision.

substantially affected by the provisions of the agreement concluded with the US, and impact on the level of protection for such data. The EDPB notes in this context that the European Commission refers to explanations given by UK authorities in recital 153 of its draft decision, without quoting or providing any concrete written assurance or commitment, nor pointing out specific legal provisions under UK law that would give effect to such explanations.

89. The EDPB has previously raised these concerns in a letter addressed to the European Parliament dated 15 June 2020[55]. The EDPB had highlighted that based on the "*EU acquis in the field of data protection, and in particular with the GDPR and the law enforcement directive*" the EDPB has reservations as to whether the safeguards in the agreement for access to personal data in the UK would apply in certain circumstances requiring disclosure obligations to the US, as well as whether these safeguards are sufficient in light of the EU standards so as to not undermine the level of protection provided in the EU.

90. Furthermore, the provisions of the UK–US CLOUD Act Agreement may significantly affect the substantive and procedural conditions under which personal data held by controllers or processors in the UK can be directly accessed by US authorities, thus impacting on the level of protection guaranteed under UK law. To provide for a level of protection essentially equivalent to the one guaranteed under EU law, it is for example "*essential that the safeguards as per such agreement include a mandatory prior judicial authorisation, as an essential guarantee for access to metadata and content data. On the basis of its preliminary assessment, the EDPB, while noting that the agreement refers to the application of domestic law, could not identify such a clear provision in the agreement concluded between the UK and the US*"[56].

91. While the European Commission highlights that data obtained under this agreement would benefit from equivalent protections to the specific safeguards provided by the so-called "EU-US Umbrella Agreement", the EDPB has concerns as to whether the incorporation of these safeguards into the UK-US CLOUD Act Agreement by a mere reference applying on a *mutatis mutandis* basis would meet the criteria of clear, precise and accessible rules when it comes to access to personal data, or would sufficiently enshrine such safeguards to be effective and actionable under UK law.

92. **The EDPB therefore recommends that the European Commission clarifies how and based on which legal instrument equivalent protections to the specific safeguards provided by the EU-US Umbrella Agreement would be given effect and have binding character under UK law.**

93. The EDPB also notes that the provisions of the UK-US CLOUD Act Agreement, read in conjunction with section 3 US CLOUD Act[57], raises questions as to the actual application of the safeguards offered by the agreement for the access, by US law enforcement authorities, to personal data in the UK processed by providers of electronic communication service or remote computing service (hereinafter "CSPs") falling under the jurisdiction of the US. Indeed, should a CSP located in the UK be subject to US law (e.g., because it is the subsidiary of a US company), it remains to be ascertained whether US authorities would be bound to rely on the UK-US CLOUD Act Agreement to obtain that data. As the European Commission points out that *"[p]articular attention will be given to the application and adaptation of the Umbrella Agreement's protections to the specific type of transfers covered by the UK-US Agreement",* the EDPB stresses that on the basis of its preliminary assessment,

[55] See EDPB response to MEPs Sophie in't Veld and Moritz Körner on the US-UK agreement under the US Cloud Act, adopted on 15 June 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0054-uk-usagreement.pdf.
[56] See the abovementioned EDPB letter.
[57] See US CLOUD Act, https://www.congress.gov/bill/115th-congress/senate-bill/2383/text.

it is unclear whether the safeguards enshrined in the UK-US CLOUD Act Agreement, and therefore the one provided by the EU-US Umbrella Agreement, would apply to all, if any, requests for access to data in the UK made by US authorities under the US CLOUD Act.

94. There may be other future international agreements or commitments with third countries the UK might be entering into in the future, and that would apply to personal data transferred from the EEA to the UK under the draft decision[58]. Depending on the provisions of these agreements and the application of specific safeguard clauses, these international agreements, by affecting the UK Data Protection Framework may also significantly impact on the substantive and procedural conditions for access to personal data in the UK by third country authorities. This is in particular the case for the draft second additional protocol to the Council of Europe Convention on Cybercrime (hereinafter "Budapest Convention") currently being negotiated among the parties to this Convention, which include several non-EU countries. Indeed, the draft protocol includes clauses which can be discretionally activated by the parties, for instance concerning the authorisation to grant access to content data or not. While all EU Member States would activate the clauses in compliance with EU data protection rules, no guarantee has been provided concerning the UK, which could substantially deviate from the level of protection that would then be offered within the EU. Another example of the issues presented above, is the Agreement between the UK and Japan for a Comprehensive Economic Partnership[59] ("CEPA"), the UK's first post-Brexit trade deal that entered into force on 1 January 2021[60] and that includes provisions on personal data[61]. The EDPB furthermore notes that the UK has also formally announced on 1 February 2021 its request to join the Comprehensive and Progressive Trans-Pacific Partnership ("CPTPP") which incorporates the Trans-Pacific Partnership Agreement ("TPP")[62].

95. The EDPB notes that, apart from the UK-US CLOUD Act Agreement, the international agreements mentioned above are not addressed in the draft decision.

96. **The EDPB invites the European Commission to:**

- **Examine the interplay between the UK Data Protection Framework and its international commitments, beyond the UK-US CLOUD Act Agreement, in particular to ensure the continuity of the level of protection in case of onward transfers to other third countries of personal data transferred from the EEA to the UK on the basis of a UK adequacy decision; and to continuously monitor and take action, where needed, with regard to the conclusion of other international agreements between the UK and third countries that risk to undermine the level of protection of personal data provided for in the EU.**

[58] See section 2.3.3 above.

[59] See UK/Japan: Agreement for a Comprehensive Economic Partnership [CS Japan No.1/2020], https://www.gov.uk/government/publications/ukjapan-agreement-for-a-comprehensive-economic-partnership-cs-japan-no12020.

[60] See UK Government's guidance on UK trade agreements with non-EU countries, https://www.gov.uk/guidance/uk-trade-agreements-with-non-eu-countries.

[61] Pursuant to Article 8.80 para. 5 CEPA, the parties commit to encourage the development of mechanisms to promote compatibility between their different legal approaches to (personal) data protection. Pursuant to Article 8.84, the parties commit not to prohibit or restrict the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person within the meaning of CEPA.

[62] Pursuant to Article 14.11 para. 2 TPP, each party shall allow the cross-border transfer of transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person.

- **Provide the EDPB with written commitments from UK authorities and identify specific provisions under UK law, in relation to the explanation related to the possible application and implementation of the UK-US CLOUD Act Agreement as referred to in recital 153 of the draft decision.**

- **Monitor, in this context, whether, in addition to the safeguards that could be provided by an appropriate implementation of the adaptation of the EU-US Umbrella Agreement, the UK -US CLOUD Act Agreement ensures appropriate additional safeguards to take into account the level of sensitivity of the categories of data concerned and the unique requirements of the transfer of electronic evidence directly by CSPs rather than between authorities.**

- **Assess the impact and potential risks of the provisions on personal data contained in international agreements recently signed by the UK, such as the CEPA.**

97. **The fifth challenge** identified relates to the application of derogations for the transfers of personal data to a third country. Although the available derogations under the UK GDPR are the same as the ones provided under the GDPR, it is important that the ICO applies and will continue to apply an interpretation in relation to the use of these derogations aligned with the one of the EDPB. If this is not the case, or if the UK diverges from this interpretation in the future, there would be a risk that the level of protection of data transferred from the EEA to third countries via the UK could be undermined.

98. **The EDPB invites the European Commission, as part of its monitoring task, to specifically check that the UK interpretation on the use of derogations remains aligned to the EU's interpretation. If however, a different interpretation of the use of derogations were followed by the UK undermining the level of protection, it is essential that the European Commission takes necessary steps by amending the adequacy decision to make sure that the level of protection provided to EEA personal data transferred to the UK will not then be undermined when these data are onward transferred from the UK to third countries on the basis of a different interpretation of derogations.**

99. **The sixth challenge,** final one for this section, refers to the absence of protections provided under Article 48 GDPR in the UK Data Protection Framework.

100. The European Commission indeed clarifies in its draft decision that in the absence of adequacy regulations or appropriate safeguards, a transfer can only take place based on derogations set out in Article 49 UK GDPR, "*with the exception of Article 48 of Regulation (EU) 2016/679 that the United Kingdom has chosen not to include in the UK GDPR."*[63] The absence of an essentially equivalent provision to Article 48 GDPR enshrined in the UK Data Protection Framework, in relation to transfers or disclosures, following a judgment of a court or tribunal or a decision of an administrative authority from another third country, may give rise to legal uncertainty as to whether the level of protection for personal data transferred from the EEA to the UK under the draft decision would be substantially affected.

101. In its GDPR Adequacy Referential, the EDPB points out that, when it comes to onward transfers, "*further transfers of the personal data by the initial recipient of the original data transfer should be permitted only where the further recipient is also subject to rules affording an adequate level of protection and following the relevant instructions when processing data on the behalf of the data*

[63] See footnote 78 of the draft decision.

controller"[64]. Furthermore, the EDPB stresses that "*the initial recipient of the data transferred from the EU shall be liable to ensure that appropriate safeguards are provided for onward transfers of data in the absence of an adequacy decision. Such onward transfers of data should only take place for limited and specified purposes and as long as there is a legal ground for that processing*"[65]. As part of Chapter V GDPR, Article 48 has to be taken fully into account in assessing whether the UK legal framework ensures an essentially equivalent level of protection in this regard[66].

102. The EDPB emphasises in this context the CJEU case-law in relation to the risk of abuse or unlawful access and use of data, stating in particular that "*as regards the level of protection of fundamental rights and freedoms that is guaranteed within the European Union, EU legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter must, according to the Court's settled case-law, lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data. The need for such safeguards is all the greater where personal data is subjected to automatic processing and where there is a significant risk of unlawful access to that data*"[67].

103. The EDPB notes in this regard that, based on the information available in the draft decision, the UK Data Protection Framework does not clearly provide that any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement in force between the requesting third country and the UK. Article 48 GDPR is an essential provision under Chapter V GDPR as it requires that a transfer or disclosure of personal data following a judgment or decision from a third country court/tribunal or administrative authority may only be recognised or enforceable if based on an international agreement in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfers pursuant to Chapter V GDPR. Indeed, the EDPB recalls that "*a request from a foreign authority does not in itself constitute a legal ground for transfer. The order can only be recognised 'if based on an international agreement such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State'*"[68]. It is therefore key that essentially equivalent provisions can be identified under UK law.

104. In the draft decision, the European Commission reports explanations from the UK authorities according to which under common law or statutes, a foreign judgment requesting data is unenforceable in the UK without an international agreement and any transfer of data upon request from a foreign court or administrative authority requires a transfer tool such as an adequacy regulation or appropriate safeguards, unless a derogation under Article 49 UK GDPR applies. However, the EDPB has not been provided with the exchanges between the European Commission and the UK authorities[69] in this regard, and is therefore not able to analyse and independently assess

[64] See WP254 rev.01, p. 6.
[65] See WP254 rev.01, p. 6.
[66] See Article 44 GDPR, last sentence, in particular: "*All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.*"
[67] See *Schrems I*, para. 91.
[68] See the annex to the EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection, adopted on 10 July 2019, https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en.
[69] See footnote 78 of the draft decision.

whether the guarantees provided by the UK authorities are sufficient to ensure an essentially equivalent level of protection in relation to the safeguards contained in Article 48 GDPR.

105. **The EDPB invites the European Commission to provide further assurances and specific references to UK legislation that ensure that the level of protection under the UK legal framework is essentially equivalent to that guaranteed within the EEA. Therefore, the EDPB invites the European Commission to provide written explanations and commitments from the UK authorities with regard to the implementation of protections essentially equivalent to those provided by Article 48 GDPR.**

106. **The EDPB considers that the identification of provisions under UK law ensuring an essentially equivalent level of protection in relation to the safeguards contained in Article 48 GDPR is all the more important in light of the concerns previously raised concerning requests for access to data in the UK made by US or other third countries' authorities, and considering that as per the adequacy decision, personal data could be transferred from the EEA to the UK without any further guarantee or binding commitment from the recipient in relation to requests for access to data by other third countries' authorities.**

3.2. Procedural and Enforcement Mechanisms

107. Based on the criteria set forth in the GDPR Adequacy Referential, the EDPB has analysed the following aspects of the UK 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 EU with the means to exercise their rights and seek redress without encountering cumbersome barriers to administrative and judicial redress.

3.2.1 Competent Independent Supervisory Authority

108. The EDPB welcomes the efforts of the European Commission to examine comprehensively the establishment, functioning and powers of the UK supervisory authority in Chapter 2.6. of the draft decision. In the UK, the Information Commissioner (hereinafter "IC") is tasked with the oversight and enforcement of the compliance with the UK GDPR and the DPA 2018. According to Schedule 12 DPA 2018, the IC is a "Corporation Sole", i.e. a separate legal entity constituted in a single person, supported by an office, the ICO.

109. With regard to the independence of the IC, the EDPB underlines that Article 51 UK GDPR does not contain the express clarification that the IC is an independent public authority as it is stated in Article 51 GDPR with regard to SAs. The EDPB nevertheless acknowledges, that the UK GDPR mirrors in its Article 52 in a similar manner the corresponding rules with regard to the independence as set forth in Article 52(1) to (3) GDPR.

110. Furthermore, the EDPB points out that Article 52 UK GDPR does not hold obligations corresponding to Article 52(4) to (6) GDPR that expressly ensure that the respective SA is provided with resources necessary for the effective performance of its tasks and exercise of its powers. The EDPB however recognises that the DPA 2018 contains provisions which aim to secure an appropriate funding of the ICO[70], as well as the circumstance that the ICO is currently one of the largest SA compared to SAs within the EU/EEA. Since an ongoing allocation of appropriate resources, especially with regard to staff and budget[71], is imperative so as to ensure the proper functioning of a SA to fulfil all of its

[70] See sections 137, 138, 182 and Schedule 12 para. 9 DPA 2018.
[71] See WP 254 rev.01, p. 7.

assigned tasks and it has also been recently flagged by the European Parliament to be of major importance[72], the EDPB deems it essential to pay particular attention to future developments in this area.

111. **Therefore, the EDPB invites the European Commission to observe any developments with regard to the allocation of resources to the ICO, which would be detrimental to the proper fulfilment of the ICO's tasks.**

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

112. The draft decision undertakes a comprehensive examination of the powers that the ICO is equipped with under Article 58 UK GDPR and the DPA 2018 in order to ensure the monitoring and enforcement of the legislation. The EDPB acknowledges that Article 58 UK GDPR mirrors in a close manner the corresponding rules with regard to powers of SAs as set forth in Article 58 GDPR. Regarding the power to impose administrative fines depending on the circumstances of each individual case, Article 83 UK GDPR contains similar provisions and maximum amounts as set forth in Article 83 GDPR. Hence, the EDPB considers the UK legal framework in this field currently to be in line with the standards as set forth in the relevant law of the EU. In that respect, the EDPB nevertheless highlights that the existence of *effective* sanctions plays an important role in ensuring respect for rules.[73]

113. **In the light of the above, the EDPB invites the European Commission to monitor the effectiveness of sanctions and relevant remedies in the UK Data Protection Framework.**

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

114. An effective supervision mechanism, allowing independent investigation of complaints so as to identify and punish infringements of data subject rights in practice, as well as an effective administrative and judicial redress (including compensation for damages as a result of the unlawful processing of data subject's personal data), are key elements for the assessment of whether a data protection system provides an adequate level of protection.

115. The EDPB welcomes that the ICO provides comprehensive information and guidelines on its website, which aim to raise awareness among controllers and processors in relation to their obligations and duties, as well as to support data subjects in order to be informed about their personal data rights and to assert their individual rights under the UK GDPR and the DPA 2018.

116. **Notwithstanding the current state, the EDPB invites the European Commission to continuously observe the level of support the ICO provides specifically to individuals, whose personal data have been transferred to the UK under the adequacy decision, to help them exercise their rights under the UK data protection regime.**

[72] European Parliament resolution of 25 March 2021 on the Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application, para. 15, https://www.europarl.europa.eu/doceo/document/B-9-2021-0211_EN.html.
[73] See WP 254 rev.01, p. 7.

4. ACCESS AND USE OF PERSONAL DATA TRANSFERRED FROM THE EU BY PUBLIC AUTHORITIES IN THE UK

4.1. Access and use by UK public authorities for criminal law enforcement purposes

4.1.1. Legal bases and applicable limitations/safeguards

117. Regarding the assessment performed by the European Commission and documented in recitals 132 and following of the draft decision **on access for law enforcement purposes**, the European Commission provides nuanced and detailed information, and generally reaches comprehensible conclusions. Therefore, the EDPB refrains from reproducing most of the factual finding and assessments in this opinion. There are, however, certain instances where the depiction of the facts or the explanation of the conclusions do not suffice in order for the EDPB to espouse them.

4.1.1.1. The use of consent

118. The EDPB takes note that the European Commission asserts in footnote 184 of the draft decision[74] that **the use of consent** is not relevant in an adequacy scenario, as in transfer situations the data are not directly collected from a data subject by a UK law enforcement authority on the basis of consent. Consequently, the use of consent as a legal basis in policing is not assessed by the European Commission.

119. In this regard, the EDPB recalls that Article 45(2)(a) GDPR requires assessing a broad array of elements not limited to the transfer situation, including "*the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including [...] criminal law*".

120. The EDPB notes, based also on the information provided by the European Commission in recital 38 of its draft implementing decision pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the UK (hereinafter "draft LED adequacy decision"), that the use of consent, as framed in the UK regime in the context of law enforcement, would always require a legal basis to be relied upon. This means that even if the police have statutory powers to process the data for the purpose of an investigation, in certain specific circumstances (for example to collect a DNA sample), the police may consider appropriate to ask for the consent of the data subject.

121. **The EDPB invites the European Commission to introduce in the adequacy decision its analysis on the possible use of consent in a law enforcement context, provided for in the draft LED adequacy decision**.

4.1.1.2. Search warrants and production orders

122. While the EDPB has no comments on the retrieval of evidence by the police through search warrants and production orders in general, it stems from recital 136 of the draft decision that the European Commission has centred its law enforcement access considerations around the police, and that the processing of personal data by other law enforcement agencies was less examined.

[74] See p. 37 of the draft decision.

123. For example, the UK Explanatory Framework for Adequacy Discussions, Section F: Law Enforcement[75], suggests on p.11 that **the National Crime Agency** (hereinafter "NCA") could be a law enforcement agency of particular interest, which *inter alia* has a wider criminal intelligence function. The NCA describes its mission as bringing together intelligence from a range of sources in order to maximise analysis, assessment and tactical opportunities, including from technical interception of communications, law enforcement partners in the UK and overseas, security and intelligence agencies[76]. The NCA is also one of the main interlocutors for the international law enforcement partners, and plays a key role in the exchange of criminal intelligence[77].

124. The EDPB further takes note of the fact that the Government Communications Headquarters (hereinafter "GCHQ"), whose activities typically fall under the scope of Part 4 DPA 2018, i.e. national security, assumes as well an active role in reducing the societal and financial harm which serious and organised crime causes to the UK, working closely with the Home Office, NCA, HM Revenue and Customs ("HMRC"), and other government departments[78]. Its activities relate to countering child sexual abuse; fraud; other types of economic crime, including money laundering; criminal use of technology; cybercrime; organised immigration crime, including people trafficking; and drugs, firearms and other illicit smuggling activity.

125. **The EDPB calls on the European Commission to complement its analysis with an analysis of the agencies active in the field of law enforcement that seem to have made collecting and analysing data, including personal data, a focus of their day-to-day operations, in particular the NCA. In addition, the EDPB invites the European Commission to have a closer look into the agencies like the GCHQ, whose activities fall both within the scope of law enforcement and national security, and the legal framework applicable to them for the processing of personal data.**

4.1.1.3. Investigatory powers for law enforcement purposes

126. Under Chapter 4 the GDPR Adequacy Referential 'Essential guarantees in third **countries for law enforcement** and national security access to limit interferences to fundamental rights', the EDPB recalls that "*[i]n this context, the court also noted critically that the previous Safe Harbor decision did*

[75] See UK Government, Explanatory Framework for Adequacy Discussions, Section F: Law Enforcement, 13 March 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf.

[76] See National Crime Agency's website, Intelligence: enhancing the picture of serious organised crime affecting the UK, https://www.nationalcrimeagency.gov.uk/what-we-do/how-we-work/intelligence-enhancing-the-picture-of-serious-organised-crime-affecting-the-uk.

[77] While not all intelligence processed by the NCA is personal data, a substantial portion might be personal information and the activities here described differ from those of classic policing, so that an assessment of access to personal data by law enforcement in the UK would be incomplete without thoroughly assessing the activities of the NCA. It seems reasonable to make sure that data protection principles are awarded the same meaning across all relevant law enforcement agencies, therefore shedding light on an especially data-driven agency such as the NCA. In addition, in "looking to the future", the explanation continues, *"[w]e continuously look for new opportunities to collect, develop and enhance traditional capabilities to increase the quantity and quality of intelligence available to exploit both in the UK and abroad." "As part of this we are developing the new National Data Exploitation Capability, using the powers vested in the agency by the Crime and Courts Act, to link together, access and exploit data held across government*." [...] "*All of this will increase our agility and flexibility to respond to new threats and operate in a proactive way, to gather and analyse information and intelligence on emerging threats so that we can take action before threats are realised*."

[78] See GCHQ's website, Mission, Serious and Organised Crime, https://www.gchq.gov.uk/section/mission/serious-crime.

*"not contain any finding regarding the existence, in the United States, of rules adopted by the State intended to limit any interference with the fundamental rights of the persons whose data is transferred from the European Union to the United States**, interference which the State entities of that country would be authorized to engage in when they pursue legitimate objectives**, such as national security*.""[79]. In this Referential, the EDPB states that the **four European Essential guarantees**[80] **need to be respected for access to data, whether for** national security purposes or **for law enforcement purposes, by all third countries in order to be considered adequate,** in particular **the necessity and proportionality with regard to legitimate objectives pursued need to be demonstrated.**

127. Under this section of the draft decision, the European Commission concludes (recital 139) "*since investigatory powers provided by the IPA 2016 are the same as those available to national security agencies, the conditions, limitations and safeguards applicable to such powers are addressed in detail in the Section on access and use of personal data by UK public authorities for national security purposes*". However it stems from the case-law of the CJEU, when applying the necessity and proportionality test to Member States' legislation allowing for retention and access to personal data by public authorities, that legitimate objectives, such as national security or fighting serious crimes, are different and, therefore, one might be able to justify a certain type of interference while the other might not[81].

128. **The EDPB would therefore welcome a specific assessment within the decision of the necessity and proportionality of the conditions, limitations and safeguards described under recitals 174 and following - which is a section devoted to measures pursuing national security objectives - when it comes to applying these conditions, limitations and safeguards in the context of a measure pursuing a law enforcement objective. It thus invites the European Commission to further clarify whether the described retention of personal data and access to it for law enforcement purposes are sufficiently limited, so as to ensure an essentially equivalent level of protection to that guaranteed within the EU.**

4.1.2. Further use of the information collected for law enforcement purposes (recitals 140-154)

129. The EDPB notes that the UK Data Protection Framework provides for similar safeguards and limitations than the ones provided under EU law in relation to the further use of the information collected for law enforcement purposes.

4.1.2.1. Further use for other law enforcement purposes

130. The DPA 2018 indeed provides that personal data collected by a competent authority for a law enforcement purpose may be further processed (whether by the original controller or by another controller) for any other law enforcement purpose, provided that the controller is authorised by law to process data for the other purpose, and the processing is necessary and proportionate to that purpose. The European Commission notes that all the safeguards provided by Part 3 DPA 2018 apply to the processing carried out by the receiving authority. The EDPB highlights however that, under Part 3 DPA 2018, sections 44(4), 45(4), 48(3) and 68(7) provide for the possibility to restrict the rights of data subject, and section 79 provides for the possibility of issuing certificates attesting that a

[79] See WP254 rev.01, p.9.
[80] See EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.
[81] See 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.

restriction is a necessary and proportionate measure to protect national security. **The EDPB therefore recommends that the European Commission further assess the possible impact of such restrictions to the level of protection of personal data in relation to the further use of the information collected. Similarly, further clarification should also be provided in relation to the UK legal framework allowing for such onward sharing, in particular the Digital Economy Act 2017, as well as the Crime and Courts Act 2013 that allows for the sharing of information with the NCA.**

4.1.2.2. Further use for other purposes than law enforcement within the UK

131. The DPA 2018 also provides that personal data collected for any law enforcement purpose may be processed for a purpose that is not a law enforcement one when the processing is authorised by law. In this case, the legal basis authorising such sharing is section 19 Counter-Terrorism Act 2008. In this regard, the EDPB notes that the scope and provisions of section 19 Counter-Terrorism Act is not fully addressed in the European Commission's assessment, and may imply further use of a broader nature, in particular as regards section 19(2) which provides that "[*i*]*nformation obtained by any of the intelligence services in connection with the exercise of any of its functions may be used by that service in connection with the exercise of any of its other functions*."

132. The EDPB also notes that the European Commission's reference to the fact that competent authorities are public authorities that must act in compliance with ECHR, including Article 8 thereof, thus ensuring that all data sharing between the law enforcement agencies and the intelligence services complies with data protection legislation, and with the ECHR, could be further substantiated by identifying the relevant acts and laws under the UK legal order laying down clearly and precisely such limits.

4.1.2.3. Further use in the context of onward transfers outside the UK

133. While the European Commission has referred to the fact that the UK-US CLOUD Act Agreement may affect onward transfers to the US from CSPs in the UK, the EDPB also highlights that the entry into force of this agreement may also affect the further use of the information collected through onward transfers from law enforcement authorities in the UK, in particular in relation to the issuance and transmission of orders as per Article 5 UK-US CLOUD Act Agreement.

134. More broadly, the EDPB considers that the conclusion of future bilateral agreements with third countries for the purpose of law enforcement cooperation, providing a legal basis for the transfer of personal data to these countries, may also significantly affect the conditions for further use of the information collected, since such agreements may affect the UK Data Protection Framework as assessed. The EDPB therefore recommends that the European Commission further assess this point, identifying the existence of international agreements, and clarifies whether the provisions of these agreements may affect the application of UK data protection law and provide for further limitation or exemption in relation to the further use and disclosure overseas of information collected for law enforcement purposes. The EDPB considers that such information and assessment are essential in order to allow a comprehensive assessment of the level of protection afforded by the UK legislative framework and practices in relation to overseas disclosure and further use.

4.1.3. Oversight

135. The EDPB notes that the oversight of criminal law enforcement agencies is ensured by a combination of different Commissioners, in addition to the ICO. The draft adequacy findings mention the IPC, the Commissioner for the Retention and Use of Biometric Material, as well as the Surveillance Camera Commissioner. In this context, it is to be noted that the CJEU has repeatedly stressed the need for independent oversight. Of particular importance on questions of access to personal data transferred

to the UK is the IPC. The understanding of the EDPB is that the IPC is a so-called "judicial commissioner", as other judicial commissioners, to be referred to in the context of the national security chapter, and that those judicial commissioners enjoy the independence of judges, also when serving as commissioners. As to the office of the IPC, the European Commission explains in recital 245 of the draft decision that it functions independently as a so-called "arm's length body", while being funded by the Home Office.

136. The EDPB has not found in the draft decision further indication to assess the independence of the Commissioner for the Retention and Use of Biometric Material, as well as of the Surveillance Camera Commissioner.

137. **The European Commission is invited to further assess the independence of the judicial commissioners, also in cases where the Commissioner is not (anymore) serving as a judge, as well as to assess the independence of the Commissioner for the Retention and Use of Biometric Material, and of the Surveillance Camera Commissioner.**

4.2. General legal framework on data protection in the field of national security

4.2.1. National security certificates

138. According to section 111 DPA 2018, controllers may apply for national security certificates issued by a Minister, member of the Cabinet, the Attorney general or the Advocate General for Scotland, certifying that exemptions from obligations and rights enshrined in Parts 4 to 6 DPA 2018 are a necessary and proportionate measure for the protection of national security. These certificates are meant to give controllers greater legal certainty, and will be conclusive evidence of the fact that national security is applicable when processing personal data. However, it should be mentioned that these certificates are not required in order to rely on national security exemptions, but instead are a measure of transparency[82].

139. The EPDB understands from Schedule 20 DPA 2018, sections 17 and 18 that a national security certificate issued under the Data Protection Act 1998 (hereinafter "old certificate") had an extended effect for the processing of personal data under the DPA 2018 until 25 May 2019. Until this date, unless replaced or revoked, the old certificates were treated as if they were issued under the DPA 2018.

140. However, where there is no express expiry date on a national security certificate issued under the Data Protection Act 1998, the EDPB understands that such a certificate will continue to have effect in relation to processing under the Data Protection Act 1998, unless the certificate is revoked or quashed[83]. Even though the protection provided by these old certificates is limited to the processing of personal data under the Data Protection Act 1998, the EDPB takes note that new national security certificates can be issued under the Data Protection Act 1998 for personal data that was processed under the Data Protection Act 1998.[84]

[82] See Home Office, The Data Protection Act 2018, National Security Certificates guidance, August 2020, para 4, p. 3, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf.
[83] See Home Office, The Data Protection Act 2018, National Security Certificates guidance, August 2020, p. 5.
[84] See Home Office, The Data Protection Act 2018, National Security Certificates guidance, August 2020, para 8, p. 5.

141. **For the sake of comprehensiveness, the EDPB invites the European Commission to clarify in its draft decision that national security certificates can still be issued under the Data Protection Act 1998. Moreover, the EDPB invites the European Commission to describe in its draft decision the redress and oversight mechanisms with regard to certificates issued under the Data Protection Act 1998. Finally, the EDPB invites the European Commission to include in its draft decision the number of existing certificates issued under the Data Protection Act 1998, and to attentively monitor this aspect.**

4.2.2. Right to rectification and erasure

142. With regard to the right to rectification and erasure, the EDPB takes note that, in accordance with section 100 and section 149 DPA 2018, data subjects have the possibility to rely on the High Court (in Scotland, the Court of Session) to order a controller to rectify or delete their data without undue delay.

143. **The EDPB stresses that the exercise of data subjects' rights needs to be effectively ensured; therefore invites the European Commission to describe in its draft decision how section 100 DPA 2018 works in practice, and to closely monitor the application of this section.**

4.2.3. Exemptions for National Security

144. The EDPB wants to draw attention to section 110 DPA 2018, and in particular to Schedule 11, which sets out the specific purposes for which intelligence services can deviate from certain data protection principles, including in relation to data subjects' rights, and are not obliged to communicate personal data breaches to the ICO.[85]

145. The **EDPB calls the European Commission to clarify further the scope of the exemptions as it wonders whether all of the exemptions provided under Schedule 11 DPA 2018 are relevant for the work of intelligence services, and whether they ensure the equivalence with the necessity and proportionality principle**. In particular, **the EDPB invites the European Commission to provide more clarification under which circumstances an intelligence service could rely on section 10 of Schedule 11 DPA 2018, which states that "*[t]he listed provisions do not apply to personal data that consists of records of the intentions of the controller in relation to any negotiations with the data subject to the extent that the application of the listed provisions would be likely to prejudice the negotiations.*"**

4.3. Access and use by UK public authorities for national security purposes

146. As a general remark, the EDPB acknowledges that States are granted a broad margin of appreciation in matters of national security, which is also recognised by the ECtHR. The EDPB also recalls that, as underlined in its updated recommendations on the European essential guarantees for surveillances measures[86], Article 6(3) Treaty on European Union establishes that the fundamental rights enshrined in the ECHR constitute general principles of EU law. However, as the CJEU recalls in its jurisprudence,

[85] These purposes are the prevention and detection of "Crime", "Information required to be disclosed by law etc or in connection with legal proceedings", "Parliamentary privilege", "Judicial proceedings", "Crown honours and dignities", "Armed forces", "Economic well-being", "Legal professional privilege", "Negotiations", "Confidential references given by the controller", "Exam scripts and marks", "Research and statistics" and "Archiving in the public interest".

[86] See EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

the latter does not constitute, as long as the EU has not acceded to it, a legal instrument which has been formally incorporated into EU law[87]. Thus, the level of protection of fundamental rights required by Article 45 GDPR must be determined on the basis of the provisions of that regulation, read in the light of the fundamental rights enshrined in the EU Charter. This being said, according to Article 52(3) EU Charter, the rights contained therein that correspond to rights guaranteed by the ECHR are to have the same meaning and scope as those laid down by the ECHR. Consequently, as recalled by the CJEU, the jurisprudence of the ECtHR concerning rights that are also foreseen in the EU Charter must be taken into account, as a minimum threshold of protection to interpret corresponding rights in the EU Charter[88]. According to the last sentence of Article 52(3) EU Charter, however, *"[t]his provision shall not prevent Union law providing more extensive protection*."

147. Therefore, in the following assessment, the EDPB has taken into account the jurisprudence of the ECtHR, to the extent that the EU Charter, as interpreted by the CJEU, does not provide for a higher level of protection which prescribes other requirements than the ECtHR case-law.

4.3.1. Legal bases, limitations and safeguards - Investigatory powers exercised in the context of national security

4.3.1.1. General remarks

148. The EDPB recalls that the IPA 2016 is a recent law that amended several provisions of the Intelligence Services Act 1994. It sets out the extent to which certain investigatory powers may be used to interfere with privacy[89]. Despite two reports of the IPC that provide useful information concerning the application of this new legal framework, there is still no review of certain aspects, in particular concerning the selectors and search criteria used.

149. Also, as a general remark concerning the IPA 2016 and its scope of application, the EDPB highlights the following four points of attention:

150. In relation to the **first point of attention**, with regard to the features of the law, the EDPB would like to underline two aspects:

151. First, the EDPB notes that the legislation refers to broad purposes for the use of procedures provided for in the IPA 2016 and not to the categories of individuals who may be concerned by the collection of data on the basis of Parts 2 to 7 IPA 2016. In this regard, the EDPB recalls that there should be a link between the categories of individuals who may be the subject of surveillance measures and the purposes pursued by the legislation to define the personal scope of the law.

152. Furthermore, the EDPB also stresses that the definition of "telecommunications operators", "telecommunications service" and "telecommunications system", which define the scope of the law, are also very broad and unclear to some extent. Indeed, the EDPB highlights that these notions, in the field of the IPA 2016, have to be understood in a much broader manner than under the telecommunications legislations, as defined for instance in the European Electronic Communications Code[90]. The EDPB notes that the definitions of "telecommunications service" and

[87] See *Schrems II*, para. 98.
[88] See 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. 124.
[89] See section 1 IPA 2016.
[90] See Article 2 (5) of the European Electronic Communications Code which defines, for instance, 'interpersonal communications service' as *"a service normally provided for remuneration that enables direct*

"telecommunication system" in the Act are said to be intentionally broad so that they will remain relevant for new technologies. Likewise, the definition of a telecommunications operator is also very broad, and could for instance include online videogames with a chat feature included, or other online websites merely including such chat windows[91].

153. In addition, whereas procedures and oversight concerning the assessment of the necessity and proportionality of collection and access to data are generally provided, the criteria to proceed to such an assessment are not defined in the law itself. Additional elements can be found in other documents, such as Codes of practice.

154. However, as recalled in the EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, the CJEU has indicated that "*the requirement that any limitation on the exercise of fundamental rights must be provided for by law implies that the legal basis which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned*"[92]. More precisely, the CJEU clarified that "*[i]n order to satisfy the requirement of proportionality, the legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data is affected have sufficient guarantees that data will be effectively protected against the risk of abuse. That legislation must be legally binding under domestic law and, in particular, must indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary*."[93]

155. The ECtHR also stressed the importance of the clarity of the law to give individuals "*an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures*"[94].

156. **The EDPB therefore calls on the European Commission to further assess these aspects concerning the preciseness, clarity and exhaustiveness of the relevant law, and to provide further elements to demonstrate it provides a level of protection essentially equivalent to that guaranteed within the EU with regard to the features of the law. The EDPB also stresses that broad definitions should also be assessed in relation to the proportionality of the interception measures.**

157. In addition, although several internal codes of the competent intelligence community authorities partly develop some of these elements, for instance concerning the assessment of the necessity and proportionality of collection of data, the EDPB stresses that the requirements of the CJEU in relation to the nature of the law imply that the core elements, including for individuals to be able to rely on

---

interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s) and does not include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service".

[91] See Home Office, Code of practice on the interception of communications, March 2018, paras 2.5 and following, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

[92] See *Schrems II*, para. 175; and the case-law cited, as well as CJEU, case C-623/17, *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others*, 6 October 2020, ECLI:EU:C:2020:790 (hereinafter "Privacy International"), para. 65.

[93] See *Privacy International*, para. 68.

[94] See ECtHR, *Zakharov v. Russia*, 4 December 2015, CE:ECHR:2015:1204JUD004714306, para. 229.

them in the context of redress, must be provided in legislation providing for actionable rights[95]. Indeed, Schedule 7, paragraph 6 IPA 2016 mentions the fact that courts (and supervisory authorities) "*take into account a failure by a person to have regard to a code in determining a question in any such proceedings*" without clarifying whether individuals can claim a breach of the codes before courts (or supervisory authorities). Moreover, the elements provided so far in the draft decision either refer to the recognition by the ECtHR of the foreseeability of the rules provided[96] in those codes, rather than to their "actionability" in court, as required by the CJEU, or to the fact that UK Courts have in some cases referred to codes, while none of the cases mentioned illustrate the possibility for individuals to action rights derived from the codes. **If it is concluded that UK law does not indicate sufficiently the circumstances and conditions under which a measure may be adopted and that these elements are in fact provided by internal codes of the intelligence community authorities**, **the EDPB would thus call on the European Commission to further assess whether the limitations and safeguards provided in the different internal codes of the intelligence community authorities may be actioned by individuals before a court and enforced.**

158. **The second point of attention** concerns the fact that the provisions relating to, on the one hand, targeted acquisition and retention of communications data and, on the other hand, to bulk collection, either in the IPA 2016 or in other legislations such as the Intelligence Services Act 1994, or the Regulation of Investigatory Powers Act 2000, will also apply to data transferred from the EU to the UK. Concerning bulk collection, the EDPB underlines that the relevant provisions of UK law allow for the collection of data outside the UK; thus could include data in transit transferred from the EEA to the UK on the basis of the adequacy decision[97]. Moreover, the EDPB notices that the European Commission indicates that "*[i]t should be noted that the retention and acquisition of communications data normally does not concern personal data of EU data subjects transferred under this Decision to the UK. The obligation to retain or disclose communications data pursuant to Part 3 and 4 of the IPA 2016 covers data that is collected by telecommunication operators in the UK directly from the users of a telecommunication service.*"[98] Nevertheless, the EDPB highlights the lack of clarity concerning the fact that only establishments of these operators situated in the UK can receive requests from the competent UK authorities since the definition of telecommunications operator provided in section 261(10) IPA 2016 requires that "a telecommunications operator is a person who offers or provides a telecommunications service to persons in the UK *or who controls or provides a telecommunication system which is (wholly or partly) in or controlled from the UK*". Consequently, personal data of EEA data subjects could actually be concerned, for instance in the case of data collected or generated by an establishment of a UK telecommunications operator located within the EEA, transferred to an establishment of this same operator situated in the UK on the basis of the adequacy decision (for commercial purposes), and then collected, within the UK, by the competent public authorities.

[95] In this regard, the CJEU considered for instance that PPD 28 in the US, did not qualify, although it provided also some limitations with regard to bulk collection, see *Schrems II*, para 181.

[96] See ECtHR, *Big Brother Watch and others v. the United Kingdom*, 13 September 2018, ECLI:CE:ECHR:2018:0913JUD005817013 (hereinafter "Big Brother Watch"), para. 325: "*As the IC Code is a public document, subject to the approval of both Houses of Parliament, and has to be taken into account both by those exercising interception duties and by courts and tribunals, the Court has expressly accepted that its provisions could be taken into consideration in assessing the foreseeability of the RIPA regime*."

[97] See para 183 and following of *Schrems II* on the assessment of a legislation providing for access to data in transit between the EU and a third country in the context of an adequacy decision.

[98] See recital 196 of the draft decision.

159. **The EDPB is therefore of the view that the assessment of these provisions are also relevant for the assessment of the level of adequacy of the UK legal framework and calls on the European Commission to clarify this aspect, and further assess to what extent this is the case. In particular, the EDPB calls on the European Commission to clarify its understanding of the scope of this legislation, including of what the notion of "users of telecommunications services" covers, and whether data from establishments of telecommunications operators outside the UK, to the extent that data of EEA data subjects are concerned, could be requested, given the very broad definition of telecommunications operators.**

160. **The third point of attention** concerns the "double-lock" procedure. The EDPB notes that a new "double-lock" procedure has been introduced in the IPA 2016. Nonetheless, the EDPB also understands that even if, in principle, collection or access to data for national security or intelligence purposes can only take place with a warrant approved by a Judicial Commissioner, the IPA 2016 provides that "*in specific limited cases lawful interception without a warrant is possible and only prior authorisation by the competent IC authorities themselves is required [see infra section on Oversight], including for interceptions in accordance with overseas requests (section 52 of the IPA 2016)*". As underlined hereafter, this also concurs to the concerns of the EDPB with regard, notably, to overseas disclosures. In addition, the EDPB also notes that for equipment interference, be it targeted or in bulk, a derogation to the double-lock procedure is also possible, and that the Judicial Commissioner is entitled to approve only the renewal of bulk warrants, after a maximum initial period of 6 months. **The EDPB calls on the European Commission to further assess and demonstrate that even in cases where the double-lock procedure does not apply, the UK legal framework provides for appropriate safeguards, including through the effective *ex post* oversight and redress possibilities offered to the individuals, to ensure that the level of protection provided is essentially equivalent to the one provided within the EU (see also infra section 4.3.3 on Oversight).**

161. Moreover, although the IPA 2016 has indeed introduced the "double-lock" procedure, the EDPB remains concerned with regard to certain features of the new legislation. Following the presentation of the corresponding sections of the draft decision, the EDPB has analysed the following types of collection and access to data in the same order as presented by the European Commission. The order of the elements assessed hereafter therefore does not reflect a hierarchy in terms of level of concern of the EDPB.

4.3.1.2. Targeted acquisition and retention of communications data

162. The EDPB notes that there are two officials who can grant targeted authorisations for obtaining communications data: the authorising officer in the Office for Communications Data Authorisations (hereinafter "the IPC"), a designated senior officer (a person holding a prescribed office or rank in a relevant public authority), in addition to the approval by a Judicial Commissioner in certain cases. However, it remains unclear for the EDPB, under the law and the relevant code, exactly which official authorises which type of targeted acquisition of communications data, and to what extent a designated officer would be sufficiently independent[99].

163. **The EDPB consequently calls on the European Commission to further assess this aspect and provide clearer explanations on these elements.**

164. Concerning the notice requiring the retention of communication data, the EDPB also notes that such notices can be addressed to a "description of operators". This notion appears to mean that several

[99] See also infra concerning the assessment of the double-lock procedure and the independence of the Judicial Commissioner.

operators can be requested at the same time to all retain data. Indeed, the targeted nature of the acquisition does not relate to the number of operators, but to the name or description of persons, organisations, location or group of persons that constitute the "target", a description of the nature of the investigation and a description of the activities for which the equipment is used. The EDPB therefore highlights that, depending on the number of operators concerned by such "description of operators", the notice may be broader than what the procedure for targeted retention may seem to imply. **The EDPB invites the European Commission to further assess this aspect, and to provide further assurances that, even when notices are addressed to several operators, they remain limited to what is strictly necessary and proportionate.**

4.3.1.3. Equipment interference

165. The EDPB notes that "equipment interference" can derogate from the double-lock procedure in case of urgency[100]. The EDPB is therefore concerned that the purposes for which such equipment interference can be required are broad, and that the criteria for urgency (in which case the Judicial Commissioner is not required to provide an *ex ante* authorisation following an assessment of the necessity and proportionality of the equipment interference) remain unclear. Since in the latter situation "the warrant ceases to have affect and may not be renewed" in case where the Judicial Commissioner does not approve the equipment interference *ex post*, the EDPB understands that the data collected meanwhile remain lawfully collected. For these data to be deleted, a specific order of the Judicial Commissioner may be issued[101].

166. **The EDPB calls on the European Commission to further assess the conditions under which urgency can be invoked, and to provide clarifications concerning the possible avenues for the exercise of rights for the data subjects concerned, and possible redress avenues offered to them in the context of equipment interference operations, especially when they take place in the context of urgency leading to a derogation to the double-lock procedure.**

4.3.1.4. Bulk interception of data from bearers

167. As described in the report of the bulk powers review[102] *"[b]ulk interception typically involves the collecting of communications as they transit particular bearers (communication links)*." The official IPA 2016 factsheet describes "bulk interception" as "*the process for the collection of a volume of communications followed by the selection of specific communications to be read, looked at or listened to where it is necessary and proportionate*." The EDPB notes that "bulk interception" of data actually implies the collection of data even before any filtering by selectors (either simple in the context of the monitoring of individuals already known to pose a threat, or complex, in the context of the identification of new threats and of previously unknown persons of interest).

168. The acquisition of bulk communications data was also one of the issues examined by the CJEU in the Privacy International case, which resulted in a judgment of the Grand Chamber issued on 6 October 2020 (in addition to whether such collection of data was performed in the context of EU law, even for national security purposes). The IPA 2016 has replaced the legislation that was the subject of this judgment.

169. The EDPB notes that, with the introduction of the IPA 2016 in UK law, a warrant is now required also to intercept data in bulk. The process to issue this warrant relies on the determination of "operational purposes". The list of these operational purposes is established by heads of intelligence services, and

[100] See section 109 IPA 2016.
[101] See section 110, subsection 3, point b) IPA 2016.
[102] See Report of the bulk powers review, by the Independent Reviewer of Terrorism Legislation, August 2016.

then approved by the Secretary of State. This decision is itself approved by an independent Judicial Commissioner who must review whether the warrant is necessary and proportionate to the operational purposes. The EDPB understands that the Judicial Commissioner does not have the power to assess the operational purposes themselves, but whether the warrant is necessary and proportionate to the operational purposes listed in the warrant. The Parliamentary Intelligence and Security Committee is provided with a copy of the list every three months, and the Prime Minister reviews the list of these operational purposes at least once a year.

170. However, on the basis of the elements provided by the European Commission in the draft decision, it appears difficult to assess the scope of these operational purposes provided in the list and whether the collection of data they allow meets the threshold set by the CJEU (for instance circumscribing the collection of data to a geographical area could be as narrow as a few streets, as well as collecting data from the EEA as a whole).

171. In addition, the EDPB underlines that data collected in bulk may be retained for long periods (to be available for further access for examination). Indeed, the EDPB notes that section 150, paragraphs 5 and 6 IPA 2016 provide only for the destruction of the copies of the data collected, and only if their retention is not necessary, or not likely to become necessary, in the interests of national security or any other grounds falling under the scope of section 138(2) IPA 2016, or if the retention is not necessary for several other purposes[103]. The EDPB stresses that these grounds appear very broad, and in any case only copies of the data obtained are mentioned.

172. Furthermore, the EDPB also notes that in urgent cases, the IPA 2016 also allows for the modification of warrants without the prior-approval of a Judicial Commissioner, and that in such case, if the Judicial Commissioner consulted *ex post* within three working days after the modification refuses to approve the modification, the warrant should have effect as if the modification had not been made, but the data collected in-between remain collected lawfully[104]. For these data to be deleted, a specific order of the Judicial Commissioner may be issued[105].

173. **The EDPB therefore calls on the European Commission for further clarifications and assessment of bulk interceptions, in particular on the selection and application of selectors in the context of these bulk interception procedures to clarify the extent to which access to personal data meets the threshold set by the CJEU (see also below section 4.3.1.7., in particular on the oversight on the selectors), and which safeguards are in place to protect the fundamental rights of individuals whose data are intercepted in this context, including concerning the retention periods of data. An independent assessment from UK competent oversight authorities would be particularly useful.**

174. **The EDPB also underlines that it seems all the more critical that "overseas-related communications" which are within the scope of bulk interception practices appear to imply that data could be directly intercepted and collected in bulk within the EEA by the UK, including for data in transit between the EEA and the UK that would fall within the scope of the draft decision (see below section 4.3.2. on further use of the information collected for national security purposes and overseas disclosure).**

[103] See subsections 3 and 6 of section 150 IPA 2016.
[104] See section 147 IPA 2016 (Part 6, chapter I).
[105] See section 181, subsection 3, point b) IPA 2016.

4.3.1.5. Protection and safeguards for secondary data

175. In addition, the EDPB is concerned that the UK relevant legislation related to bulk interception does not provide for the same level of protection to all communications data. "Secondary data", which can be obtained with a bulk warrant are, according to section 137 IPA 2016, both "systems data", "*which is comprised in, included as part of, attached to or logically associated with the communication (whether by the sender or otherwise)*", and "identifying data", "*which is comprised in, included as part of, attached to or logically associated with the communication (whether by the sender or otherwise), is capable of being logically separated from the remainder of the communication, and if it were so separated, would not reveal anything of what might reasonably be considered to be the meaning (if any) of the communication, disregarding any meaning arising from the fact of the communication or from any data relating to the transmission of the communication*"[106].

176. The EDPB notes that these "secondary data", also known as "metadata"[107], collected in bulk, seem not to benefit from the same safeguards as data collected with a targeted warrant, but also as content data collected in bulk. Indeed, the EDPB notices that the selection of any of the intercepted content benefits from more safeguards[108] than the selection of secondary data[109].

177. Furthermore, the EDPB stresses that both the ECtHR[110] and the CJEU[111] have questioned the fact that such data are less sensitive than others, and in particular than content data. Indeed, the Code of Practice concerning interceptions presents as examples of "secondary data" (both "systems data" such as router configurations, email addresses or users ID; but also alternative account identifiers, as well as "identifying data", such as the location of a meeting in a calendar appointment, photograph information, such as the time, date and location when it was taken). **The EDPB thus stresses the consistent assessment by the ECtHR and the CJEU, and recalls the concerns expressed in relation to secondary data that should benefit from specific safeguards due to their sensitivity. The EDPB**

[106] "Systems data" and "identifying data" are defined in section 263 IPA 2016.
[107] See Report of the bulk powers review, by the Independent Reviewer of Terrorism Legislation, August 2016.

[108] See section 152, subsection 1, point c) and subsections 3 and following IPA 2016.
[109] See section 152, subsection 1, points a) and b) IPA 2016.
[110] See ECtHR, *Big Brother Watch*, para. 357, under referral to the Grand Chamber: "*Consequently, while the Court does not doubt that related communications data is an essential tool for the intelligence services in the fight against terrorism and serious crime, it does not consider that the authorities have struck a fair balance between the competing public and private interests by exempting it in its entirety from the safeguards applicable to the searching and examining of content. While the Court does not suggest that related communications data should only be accessible for the purposes of determining whether or not an individual is in the British Islands, since to do so would be to require the application of stricter standards to related communications data than apply to content, there should nevertheless be sufficient safeguards in place to ensure that the exemption of related communications data from the requirements of section 16 of RIPA is limited to the extent necessary to determine whether an individual is, for the time being, in the British Islands..*"
[111] See CJEU, *Privacy International*, 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).*"

therefore calls on the European Commission to carefully assess whether the safeguards provided under UK law for such category of personal data ensure an essentially equivalent level of protection to the one guaranteed in the EU.

4.3.1.6. Automated processing of communications data

178. The EDPB notes that intelligence community authorities do not only use simple or complex selectors to filter the data acquired in bulk, but that they may also rely on other automated processing tools to analyse "*large volumes of information, which enables the Agencies also to find linkages, patterns, associations or behaviours which might demonstrate a serious threat requiring investigation*", according to the Intelligence and Security Committee report 2015[112]. **The EDPB is aware of the fact that this public report concerns practices under the previous legal framework, which was subsequently replaced by the IPA 2016. Nevertheless, it sees a need for further independent assessment and oversight of the use of automated processing tools by the competent UK oversight authorities, and calls on the European Commission to further assess this issue and the safeguards that would and/or could be afforded to EEA data subjects in this context**.

4.3.1.7. Compliance risks and incompliant practices of competent Intelligence Community authorities

179. The EDPB takes note that detailed oversight reports are available. They provide for valuable elements as to what they assess as positive compliance practices, as well as to the compliance risks and incompliant practices identified.

180. In this regard, according to the IPC in its report for 2019, several elements concerning the application of the legal framework by the different competent authorities have revealed some (risks of) incompliances by the competent authorities.

181. First, the EDPB has noticed that the criteria to classify a dataset as bulk personal dataset or as targeted data do not seem to be always clear for the MI5 and SIS themselves, in particular for the MI5, which can lead to the absence of appropriate safeguards applied to the data[113]. In its report on 2019, the IPC suggested that "*this question should be resolved as a priority*"[114]. Also in relation to bulk personal datasets, the EDPB notes that for the GCHQ, although the classification of bulk personal datasets seems to be satisfying (but yet remains to be audited by the IPC), in March 2019, the internal compliance review of warrants by the dedicated team raised serious concerns, with 50% of the justifications for bulk acquisition warrants that were reviewed by the GCHQ compliance team that did not meet the required standard. According to the IPC, the compliance team had begun work to

---

[112] See Intelligence and Security Committee of Parliament, Privacy and Security: A modern and transparent legal framework, 2015, para. 18, p. 13, https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf.

[113] See Annual Report of the Investigatory Powers Commissioner 2019, 15 December 2020, point 8.39, https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPC-Annual-Report-2019_Web-Accessible-version_final.pdf: "*We have observed the positive development of the [Bulk Oversight Panel (BOP)] and note its impact in managing internal compliance. We continue to seek greater clarity regarding the process MI5 uses to carry out initial examinations of new data sets to better understand decisions to classify a dataset as BPD or, for example, as targeted data. We were concerned by one unresolved action on the BOP minutes around resolving discrepancies between allocations of BPD between MI5 and SIS. It is possible, because of the different uses of the data and the different cuts of data being held, that both agencies could hold the same dataset, or versions of it, and that it could lawfully be categorised as bulk by one and targeted data by the other. There is a risk that, if one of the agencies has incorrectly categorised the data holding as targeted then that data would be held without appropriate warrant and might not be subject to appropriate safeguards*."

[114] See Annual Report of the Investigatory Powers Commissioner 2019, point 8.39.

investigate the problem and retrain staff to improve this standard. The refreshed training on the IPA 2016 provisions and the additional training provided by policy and compliance networks (hereinafter "PCNs") have improved GCHQ's compliance in this area. The IPC does not expect to see a slip in this standard at future inspections, but will continue to review this area closely[115]. **The EDPB therefore shares the view that further review and monitoring of the said elements by the European Commission is needed as part of the assessment of the level of protection to ensure that this standard is improved, as underlined in the IPC's report, and recalls that implementation and concrete application of the legal framework shall also be taken into account as provided under Article 45 GDPR when assessing the essential equivalence of a third country.**

182. More broadly, the EDPB stresses the points of attention shared by the IPC concerning the "task-based searches" led by the MI5 officers – which allows an investigator to conduct more than one search of the bulk personal data sets available to them, and the "*serious compliance risks associated with certain technology environments in use by MI5*", concerning where data were stored in the environment, who had access to them, the extent to which they were being copied or shared, the deletion processes which applied to them, as well as concerning retention periods. Although the IPC indicates that measures have been taken and safeguards introduced, some of them remain manual and led on an individual, human-basis, it highlights that it is critical that the *"MI5 continues to maintain these new processes and to provide sufficient resources for them to function effectively. If MI5 identifies an increase in non-compliant behaviours*"[116]. The IPC expects they would be brought to its attention as soon as possible. **The EDPB therefore calls on the European Commission to closely monitor these aspects in the future**.

183. Concerning the GCHQ, the EDPB also understands from the report of the IPC that, for operations conducted under the bulk warrants, "*the quality of applications for internal approval was variable and we observed that there was room for improvement in the way that such applications were set out*"[117], and that for targeted equipment interference, the explanations for the use of general descriptors were sometimes too general and imprecise[118]. The EDPB also noticed that in the context of bulk equipment interference, the IPC recommends that "*applications should consistently and explicitly record the link between the target and a statutory purpose and intelligence requirements*"[119], that "*all applications should clearly address the potential for collateral intrusion and relevant mitigations when assessing proportionality*"[120], and that the IPC stressed that despite progress, "*there is still room for improvement*"[121] and further attention will be needed as well in the future.

184. In relation to the bulk interception regime under the Regulation of Investigatory Powers Act 2000 (hereinafter "RIPA 2000") which has since been replaced by provisions in the IPA 2016, the EDPB recalls that the insufficient oversight, both of the selection of Internet bearers for interception and the filtering, search and selection of intercepted communications for examination, was one of the core aspects that the ECtHR deemed incompliant with Article 8 ECHR with regard to the previous legislation on the investigatory powers of UK authorities in the context of national security in the *Big Brother Watch* case, now referred to the Grand Chamber. **The EDPB invites the European**

[115] See Annual Report of the Investigatory Powers Commissioner 2019, point 10.48.
[116] See Annual Report of the Investigatory Powers Commissioner 2019, point 8.52.
[117] See Annual Report of the Investigatory Powers Commissioner 2019, point 10.2.
[118] See Annual Report of the Investigatory Powers Commissioner 2019, points 10.16 and 10.17.
[119] See Annual Report of the Investigatory Powers Commissioner 2019, point 10.23.
[120] See Annual Report of the Investigatory Powers Commissioner 2019, point 10.23.
[121] See Annual Report of the Investigatory Powers Commissioner 2019, point 10.23.

Commission to verify the state of play of the proceedings, to take these elements into account, and to specify them in the adequacy decision should the European Commission adopt it.

185. In this case, the ECtHR was: "*not persuaded that the safeguards governing the selection of bearers for interception and the selection of intercepted material for examination are sufficiently robust to provide adequate guarantees against abuse. Of greatest concern, however, is the absence of robust independent oversight of the selectors and search criteria used to filter intercepted communications*."[122] As highlighted by the IPC*, "this finding echoed a similar recommendation in the Intelligence and Security Committee's Privacy and Security: A modern and transparent legal framework report of March 2015"*[123]. **The EDPB welcomes the fact that consequently, the IPC conducted a review of its approach to inspecting bulk interception in 2019, "*which included a careful review of the technically complex ways in which bulk interception is actually implemented*"[124] and committed to include "*a detailed examination of the selectors and search criteria alluded to above by the ECtHR*"[125] in the inspections of bulk interception from 2020 onwards. Given the importance of this aspect, the EDPB is concerned that a detailed examination of the selectors and search criteria by the IPC has not been carried out yet, and calls on the European Commission to closely monitor developments in this regard, especially since the concrete format of such oversight remains to be clarified[126].**

4.3.2. Further use of the information collected for national security purposes and overseas disclosure

186. When it comes to the further use of the information collected for national security purposes, the European Commission refers in its assessment to section 87(1) DPA 2018, which indeed provides that "*personal data so collected must not be processed in a manner that is incompatible with the purpose for which it is collected*". The EDPB however points out that this provision may be subject to national security exemptions as per section 110 DPA 2018. The EDPB furthermore notes that, whether for targeted interception and examination, for targeted acquisition and retention of communications data, for targeted equipment interference or for bulk interception and bulk equipment interference, the legislation provides for the possibility of "overseas disclosure".

4.3.2.1. Further use, overseas disclosure and the applicable legal framework in the UK

187. The European Commission has identified Part 4 DPA 2018, and in particular its section 109 as relevant provisions setting out specific requirements for the further use of the information collected, and notably the international transfer of personal data by intelligence services to third countries or international organisations. However, the EDPB notes that section 110 DPA 2018 provides for a national security exemption specifying that certain provisions of the DPA 2018 do not apply if exemption from these provisions is required for the purpose of safeguarding national security. The concerned provisions that may not apply include chapter 2 of Part 4 DPA 2018 in relation to the data protection principles, including purpose limitation, as well as chapter 3 of Part 4 DPA 2018 in relation to data subject rights. Section 109 DPA 2018, read in conjunction with section 110 DPA 2018 and the conditions under which it applies may lead to cases where an international transfer of personal data

[122] See ECtHR, *Big Brother Watch*, para. 347.
[123] See Annual Report of the Investigatory Powers Commissioner 2019, point 10.28.
[124] See Annual Report of the Investigatory Powers Commissioner 2019, point 10.28.
[125] See Annual Report of the Investigatory Powers Commissioner 2019, point 10.28.
[126] See Annual Report of the Investigatory Powers Commissioner 2019, point 10.28: "the exact format of this inspection is yet to be agreed".

by intelligence services to third countries takes place without applying provisions related to the data protection principles and data subject rights.

188. As identified by the European Commission, such exemption must be assessed case-by-case, and can be invoked only as far as the application of a particular provision would have negative consequences for national security. Indeed, the issuance of a national certificate for the UK intelligence services aims at certifying that an exemption is required in respect of specified personal data that are processed for the purpose of safeguarding national security. The EDPB however notes that in its guidance for national security certificate under the DPA 2018, the UK Home Office clarifies that "*[i]t is important to note from the outset that a certificate is not required in order to rely on the national security exemption; in fact, in most cases, controllers will determine for themselves whether the national security exemption is applicable*." [127] Furthermore, the UK Home Office guidance notes that "*national security certificates may apply to personal data which can be specifically identified or cover a broader category of personal data. They may be pre-emptive as well as retrospective*." [128] National security exemption may therefore apply in relation to an international transfer of personal data by intelligence services to third countries in the absence of a national security certificate.

189. The EDPB furthermore notes that, for example, the national security certificate DPA/S27/Security Service[129] provides that until 24 July 2024, personal data processed "*for, on behalf of, at the request of or with the aid or assistance of the Security Service or*" and "*where such processing is necessary to facilitate the proper discharge of the functions of the Security Service described in section 1 of the Security Service Act 1989*" are exempted from the corresponding provisions in UK law to Chapter V GDPR in relation to transfers of personal data to third countries or international organisations. While the other national security certificates publicly available do not provide for an exemption from the provisions of section 109 DPA 2018, it is to be recalled that some or all of the text of a national security certificate may be withheld if its publication would be against the interests of national security, would be contrary to the public interest, or might jeopardise the safety of any person.

190. In general, while assessing the draft decision in relation to these provisions, the EDPB observes that the safeguards for these disclosures solely comprise the requirement that the recipient of the data respects requirements concerning the security of data, the extent of the disclosure limited to what is necessary, the retention of data and the restriction of access to data to a limited number of persons. Thus, **the EDPB underlines that when it comes to overseas disclosures, the application of the national security exemption provided under UK law may lead to situations where safeguards ensuring that the principles of purpose limitation, necessity and proportionality, as well as the rights for the individuals, oversight and redress would not be fully provided or respected in the third country of destination. The EDPB therefore recommends the European Commission to further examine the overall safeguards provided under UK law when it comes to overseas disclosure, in particular in light of the application of national security exemptions.**

4.3.2.2. Overseas disclosure and intelligence sharing in the context of international cooperation

191. The EDPB also notes that the European Commission did not consider, as part of its adequacy assessment, existing international agreements concluded between the UK and third countries or

[127] See Home Office, The Data Protection Act 2018, National Security Certificates guidance, August 2020, para 3, p. 3.
[128] See Home Office, The Data Protection Act 2018, National Security Certificates guidance, August 2020, para 5, p. 4.
[129] See DPA/S27/Security Service, section 27 DPA 2018, Certificate of the Secretary of State, 24 July 2019, https://ico.org.uk/media/about-the-ico/documents/nscs/2615660/nsc-part-2-mi5-201908.pdf.

international organisations that may provide for specific provisions for the international transfer of personal data by intelligence services to third countries.

192. The EDPB also stresses that the European Commission's assessment mainly relies on the assessment of Part 4 DPA 2018, and is notably concerned that the IPA 2016 focuses on 'requests' to exchange intelligence with foreign partners, but does not address other forms of intelligence sharing. The EDPB notes in this regard that the European Commission draft decision does not refer or assess the articulation between the UK legislative framework with the "UK-US Communication Intelligence Agreement" ("UK-US CI Agreement"). In a recent statement marking the 75th Anniversary of this agreement, the US National Security Agency (hereinafter "NSA") mentioned that this partnership allows "*to share information between the two agencies as much as possible, with minimal restrictions*" and that "*this ground-breaking document created the policies and procedures for UK and US intelligence professionals for sharing communication, translation, analysis, and code breaking information*."[130] This agreement also became the foundation for other intelligence partnership with Australia, Canada, and New Zealand.

193. The secret nature of this agreement and its specific provisions raise a serious challenge in terms of clarity and foreseeability of the law in relation to the further use and overseas disclosure of information collected by UK authorities for national security purposes. In this context, the EDPB recalls that when it comes to the level of protection guaranteed within the EU, the CJEU has stressed that legislation involving interference with the fundamental right to the protection of personal data must "*lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data. The need for such safeguards is all the greater where personal data is subjected to automatic processing and where there is a significant risk of unlawful access to that data*"[131]. The EDPB therefore considers that the European Commission should consider the impact of the UK-US CI Agreement as part of its adequacy assessment.

194. The ECtHR, in its first section judgment of 13 September 2018, in the *Big Brother Watch* case, has assessed the UK intelligence sharing regime and in particular the UK-US CIAgreement. The ECtHR indeed stated that "*[t]he statutory framework which permits the United Kingdom intelligence services to request intercepted material from foreign intelligence agencies is not contained in RIPA. The British-US Communication Intelligence Agreement of 5 March 1946 specifically permits the exchange of material between the United States and the United Kingdom"*[132] and considered that there is *"a basis in law for the requesting of intelligence from foreign intelligence agencies, and that that law is sufficiently accessible*."[133] While the ECtHR has concluded that there has been no violation of Article 8[134] ECHR in relation to the intelligence sharing regime, the EDPB notes that this judgment has now been referred to the Grand Chamber which decision is still pending. The EDPB also notes that in a partly concurring, partly dissenting opinion to this judgment, Judge Koskelo, joined by Judge

[130] See NSA's press release, GCHQ and NSA Celebrate 75 Years of Partnership, 5 February 2021, https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2494453/gchq-and-nsa-celebrate-75-years-of-partnership/.
[131] See *Schrems I*, para. 91.
[132] See ECtHR, *Big Brother Watch*, para. 425.
[133] See ECtHR, *Big Brother Watch*, para. 427.
[134] See ECtHR, *Big Brother Watch*, para. 448.

Turković[135], has concluded that there is a violation of Article 8 ECHR in relation to the intelligence sharing regime, stating that "*[i]t is easy to agree with the principle that any arrangement under which intelligence from intercepted communications is obtained via foreign intelligence services, whether on the basis of requests to carry out such interception or to convey its results, should not be allowed to entail a circumvention of the safeguards which must be in place for any surveillance by domestic authorities (see paragraphs 216, 423 and 447). Indeed, any other approach would be implausible*".

195. As highlighted by several reports from the media and non-governmental organisations[136][137], the most recent version of the UK-US CI Agreement to have been made public dates back from 1956 and since then, communication technology and the nature of signals intelligence have changed significantly. Media reports have for example revealed that data transiting through undersea cables that land in the UK are intercepted by the GCHQ and made accessible to the NSA[138].

196. For the EDPB, a key question in relation to intelligence sharing is whether section 109 DPA 2018 and the provisions of the IPA 2016 remain applicable when UK intelligence services act in accordance with the UK-US CI Agreement. Another key element to be assessed is whether the provisions or effective application of this agreement impact on the level of protection of personal data in transit from the EEA to the UK, or allows for a direct access and acquisition of personal data by other third countries intelligence services.

197. Consequently, in addition to reservations expressed as to "overseas disclosures" on the basis of Part 4 DPA 2018 and its related national security exemption, as well as of requests in the framework of the IPA 2016, **the EDPB is concerned about other forms of information-sharing and disclosures, on the basis of other instruments, in particular the various international agreements concluded by the UK with other third countries, especially where these instruments remain inaccessible to the public, such as the UK-US CI Agreement. The effect of such agreement could lead to a circumvention of the safeguards identified in relation to the access and use of personal data for national security purposes.**

198. Indeed, the EDPB shares the view expressed by Special Rapporteur to the United Nations, Joe Cannatacci, that "*[i]ntelligence sharing must not result in a backdoor to obtain or facilitate for others the obtaining of intelligence free from domestic safeguards, nor a loophole for foreign Governments with lower standards on the protection of privacy (or other human rights) to obtain intelligence from UK intelligence that could give rise to human rights violations*"[139].

199. Furthermore, **the EDPB considers that the conclusion of bilateral or multilateral agreements with third countries for the purpose of intelligence cooperation, providing a legal basis for direct interception and acquisition of personal data or the transfer of personal data to these countries**

---

[135] See ECtHR, *Big Brother Watch*, partly concurring, partly dissenting opinion of Judge Koskelo, joined by Judge Turković.

[136] See BBC, Diary reveals birth of secret UK-US spy pact that grew into Five Eyes, 5 March 2021, https://www.bbc.com/news/uk-56284453.

[137] See Privacy International, Policy Briefing - UK Intelligence Sharing Arrangements, April 2018, https://privacyinternational.org/sites/default/files/2018-04/Privacy%20International%20Briefing%20-%20Intelligence%20Sharing%20%28UK%29%20FINAL.pdf.

[138] See The Guardian, GCHQ taps fibre-optic cables for secret access to world's communications, 21 June 2013, https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

[139] See End of Mission Statement of the Special Rapporteur on the Right to Privacy at the Conclusion Of his Mission to the United Kingdom of Great Britain and Northern Ireland, London, 29 June 2018, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E#:~:text=Intelligence%20sharing%20must%20not%20result,UK%20intelligence%20that%20could%20give.

may also significantly affect the conditions for further use of the information collected, since such agreements are likely to affect the UK data protection legal framework as assessed.

4.3.3. Oversight

200. The EDPB emphasises the importance of comprehensive supervision by independent supervisory authorities for an adequate level of data protection. The guarantee of independence within the meaning of Article 8(3) EU Charter of the supervisory authorities 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.

201. When personal data are accessed and used for national security purposes, the oversight function is mainly fulfilled by the IPC and the Judicial Commissioners (hereinafter the "Judicial Commissioners").

202. **The EDPB generally recognises the introduction of Judicial Commissioners in the IPA 2016 as a significant improvement.** In line with a request above, the European Commission is invited to assess the independence of the **Judicial Commissioners in more detail, and in particular to what extent the independence of the IPC and the IPC's office (hereinafter "IPCO") is legally secured, as such is not found in the IPA 2016.** This is even more important as the IPC decides on appeals by the government, in case an application for a surveillance **measure** has been denied **by** a judicial commissioner.

203. The IPC has *ex-ante*, as well as *ex-post* oversight functions. As regards *ex-ante* oversight, the EDPB understands that the function of the Judicial Commissioners is to approve, in individual cases, different surveillance measures, including targeted interception and bulk acquisition of communication data. The EDPB further notes that prior-approval of surveillance measures cannot be derived from the jurisprudence of the CJEU as an absolute requirement for the proportionality of surveillance measures.[140]

204. In order to assess the effectiveness of this level of oversight, the EDPB nevertheless sees the need to further clarify the scenarios for which a lawful interception without a prior-approval of the Judicial Commissioners is possible.

205. In its draft decision, the European Commission mentions in footnotes 201 and 266 "specific limited cases" provided by the IPA 2016 in its sections 44 to 52 with regard to targeted interceptions. The EDPB notes that sections 45 - 51 IPA 2016 are exemptions that are claimed not to be regularly used by intelligence services. Furthermore, the **EDPB understands** that in the **cases where the exemptions apply** (e.g. telecommunications and postal providers), the prior-approval carried out by the Judicial Commissioners is to be conducted in the event that law enforcement authorities or intelligence services **request** access to these data**, and invites the European Commission to confirm in its decision that this is correct**.

206. The EDPB recognises that section 44(2) IPA 2016 permits interception of communications if one of the parties (sender or recipient) has consented and there is an authorisation under the RIPA 2000 or the Regulation of Investigatory Powers (Scotland) Act 2000 (2000 asp 11), i.e. the former legal situation before the establishment of the Judicial Commissioners. The EDPB **invites** the European

[140] It also notes, however, that the CJEU, when invalidating the Privacy Shield in *Schrems II*, has taken note of the fact that, under US law, the so called FISA Court "*does not authorise individual surveillance measures; rather, it authorises surveillance programs (like PRISM, UPSTREAM) on the basis of annual certifications*"." (para. 179).

Commission to clarify whether this means that in cases where a unilateral consent exists, the prior-approval procedure would not apply at all.

207. As regards *ex-post* oversight, it is also important to verify that efficient independent oversight is ensured without gaps, in particular where it is not foreseen *ex-ante*.

208. The EDPB notes that for the sections 48 - 52 IPA 2016, an *ex-post* review by the Judicial Commissioners takes place, and **invites the European Commission to clarify under which requirements and on whose initiative such an *ex-post* review is to be conducted**.

209. According to section 229(4) IPA 2016, the IPC is not to keep under review the exercise of certain functions. In this regard the EDPB invites the European Commission to clarify the provisions of section 229(4)(d) and (e) IPA 2016 regarding its practical impact on the review competence of the IPC. **It is the understanding of the EDPB that the ICO is the competent oversight authority where the exemptions of section 229(4) IPA 2016 apply, and the EDPB invites the European Commission to confirm in its decision that this is correct.**

210. **It appears that, when conducting** *ex-post* oversight**, the IPC's** role is **limited** to make recommendations in cases of non-compliance, and to give notice to the data subject, if the error is serious and it is in the public interest for the person to be informed. **The EDPB invites the European Commission to clarify how the IPCO can effectively ensure compliance with the law.**

211. **Finally, the EDPB understands that affected individuals cannot directly address the IPCO, but must lodge a complaint with the ICO, which, however, has limited competences in the area of national security. The EDPB therefore invites the European Commission to further clarify how it is legally ensured that the IPCO addresses complaints in these cases.**

4.3.4. Redress

212. In the light of the *Schrems I* and *Schrems II* judgments by the CJEU, it is clear that effective judicial protection in the meaning of Article 47 EU Charter is of fundamental importance for the assumption of adequacy of the law of a third country. The rulings have also shown that particular attention, in this regard, has to be paid to effective judicial protection in the area of national security access to personal data.

213. **The EDPB recognises that the UK has established the IPT. The IPT is not only competent to hear cases on the use of investigatory powers by law enforcement authorities, but also by intelligence services. It is the understanding of the EDPB that the IPT functions as a proper court in the meaning of Article 47 EU Charter. As to its powers, the European Commission is invited to confirm that the IPT has all those powers mentioned in recital 262 of the draft decision, regardless of the legal basis under which the complaint is brought.**

214. Discreet surveillance by intelligence agencies will often mean that the object of the surveillance, the data subject, is and will not be aware of the surveillance. In this context, when it had to analyse US law, the EDPB has many times expressed its concern with the requirement of "standing", as interpreted in US law, in surveillance cases. Against this background, the EDPB notes that the complaint with the IPT only requires a "belief" test, according to which the complainant has to show she or he is potentially at risk of being subjected to a measure.

215. When analysing the IPT, the EDPB also pays particular attention to the fact that the functioning of the IPT has been repeatedly found to be in compliance with the ECHR, as interpreted by the ECtHR.