Opinion 15/2021 regarding the European Commission Draft Implementing Decision pursuant to Directive (EU) 2016/680 on the adequate protection of personal data in the United Kingdom

Adopted on 13 April 2021

Version history

Version 1.1	06 July 2021	Formatting change
Version 1.0	13 April 2021	Adoption of the Opinion

CONTENTS

The European Data Protection Board

Having regard to Article 51(1)(g) of Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA[1] (hereinafter "LED"),

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 LED 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 has used as main reference for this work its LED Adequacy Referential[4] adopted on 2 February 2021, as well as the relevant case-law reflected in the EPDB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures[5].

4. 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.

5. However, the EDPB recalls that, to be considered as providing an adequate level of protection, Article 36 LED 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 LED. In the area of data protection, the EDPB notes that there is a strong alignment between the LED 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

[1] OJ L 119, 4.5.2016, p. 89.
[2] See European Commission's press Release, 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 EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, adopted on 2 February 2021, https://edpb.europa.eu/sites/edpb/files/files/file1/recommendations012021onart.36led.pdf_en.pdf.
[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.

retention, security and confidentiality; transparency; special categories of data; automated decision making and profiling.

6. The EDPB recommends that the European Commission complement its analysis with information about the existence of a mechanism to inform the relevant Member States' competent authorities of further processing or disclosure by the UK authorities to which they transferred the personal data and identify its effectiveness under the UK legal order.

7. The EDPB considers that the provisions under Chapter 5 of Part 3 Data Protection Act 2018 (hereinafter "DPA 2018"), do, in principle, provide for a level of protection that is essentially equivalent to the one guaranteed under EU law, when it comes to transfer of personal data from a UK law enforcement authority to a third country.

8. 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 this might lead to possible risks in the protection provided to personal data transferred from the EU especially if, in the future, the UK data protection framework deviates from the EU acquis. **For the above situations, the European Commission should therefore fulfil its monitoring role, and in case the essentially equivalent level of protection of personal data transferred from the EU is not maintained, the European Commission should consider amending the adequacy decision to introduce specific safeguards for data transferred from the EU, and/or to suspend the adequacy decision.**

9. **Finally, 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, 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.

10. In this regard, the EDPB highlights that the entry into force of the Agreement between the UK and the US on Access to Electronic Data for the Purpose of Countering Serious Crime (hereinafter "UK-US CLOUD Act Agreement")[6] may affect onward transfers from law enforcement authorities in the UK, in particular in relation to the issuance and transmission of orders as per Article 5 of the UK-US CLOUD Act Agreement.

11. The EDPB also recommends that the European Commission continuously monitors whether the conclusion of future agreements with third countries for the purpose of law enforcement cooperation, providing a legal basis for the transfer of personal data to these countries, could affect the conditions for onward sharing of the information collected, in particular whether the provisions of these international 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 review of the level of protection afforded by the UK legislative framework and practices in relation to overseas disclosure.

[6] 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.

2 INTRODUCTION

2.1 UK data protection framework

12. The UK data protection framework is largely based on the EU data protection framework (in particular the LED and 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 (hereinafter "GDPR")), which derives from the fact that the UK was a Member State of the EU up until the 31 January 2020. Moreover, the DPA 2018, which came into force on 23 May 2018 and repealed the UK Data Protection Act 1998, transposes the LED through Part 3 thereof, in addition to further specifying the application of the GDPR in UK law, as well as granting powers and imposing duties on the national data protection supervisory authority, the UK Information Commissioner's Office (hereinafter "ICO").

13. As mentioned in recital 12 of the 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 to the UK's withdrawal from the EU to fit the domestic context.

14. Consequently, the relevant legal framework applicable in the UK after the end of the transition period[7] 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 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 Investigatory Power Act 2016 ("IPA 2016").

(together "the UK Data Protection Framework").

2.2 Scope of the EDPB's assessment

15. 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 51(1)(g) LED, 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.

16. As mentioned in the LED 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* [8]".

[7] 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 EU to the UK is not deemed a transfer.

[8] See Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, para 15, p. 5.

17. 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[9].

18. 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. 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.

19. The EDPB took into account the applicable European data protection framework, including Articles 7, 8 and 47 of the Charter of Fundamental rights of the European Union (hereinafter "the 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 LED, as well as the relevant case-law.

20. The objective of this exercise is to provide the European Commission with an opinion for 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"[10]. Therefore, the objective is not to mirror point by point the European legislation, but to establish the essential and core requirements of the legislation under examination. Adequacy can be achieved through a combination of rights for the data subjects and obligations on those who process 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

[9] These are the elements where the European Commission refers, in its draft decision, to explanations from the UK authorities without providing the written documents from the UK authorities supporting the explanations, such as with regard to: the effects of the transitional provisions and the absence of a "sunset" provision (recital 87); examples of consent as an appropriate basis for the processing (footnote 68); the term "inaccurate" as "incorrect or misleading" personal data (footnote 79); the remit of ISC (footnote 245); the low threshold for making a complaint with the IPT and the fact that it is not unusual for the IPT to determine that the complainant was in fact never subject to investigation by a public authority (footnote 263); the combination of powers derived from the legislation and common law (footnote 52); the prerogative powers exercised by the government (footnote 62); the fact that other organisations are free to follow the MoPI Code of Practice principles if they wish (footnote 86).

[10] 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.

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[11].

2.3 General comments and concerns

2.3.1 International commitments entered into by the UK

21. According to Article 36 (2) (c) LED and the LED Adequacy Referential[12], when assessing the adequacy of the level of protection of a third country, the European Commission shall take into account, among others, the international commitments the third country has entered into, or other obligations arising from the third country's participation in multilateral or regional systems in particular in relation to the protection of personal data, as well as the implementation of such obligations. 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")[13] and its Additional Protocol[14] should be taken into account.

22. **In this regard, the EDPB welcomes that the UK has adhered to the ECHR and is under the jurisdiction of the European Court of Human Rights ("ECtHR"). In addition, the UK has also adhered to Convention 108 and its Additional Protocol, has signed Convention 108+[15] in 2018 and is currently working on its ratification.**

2.3.2 Possible future divergence of UK Data Protection Framework

23. As mentioned in recital 171 of the draft decision, the European Commission must take into account that, with the end of the transition period provided by the Withdrawal Agreement[16], the UK administers, applies and enforces its own data protection regime and as soon as the bridge provision[17] under Article FINPROV.10A of the EU-UK Trade and Cooperation Agreement[18] 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.

[11] See EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, para. 14, p. 5.
[12] See EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, para 24, p.7.
[13] See Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, Convention 108, 28 January 1981.
[14] 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.
[15] See Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter "Convention 108+"), 18 May 2018.
[16] 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).
[17] 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 EU to the UK is not deemed a transfer.
[18] 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).

24. The European Commission has therefore decided to include a sunset clause in its draft decision[19], setting the expiration date four years after its entry into force.

25. 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.

26. 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[20].

27. **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[21]. 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.**

28. 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"), and in particular regarding complaints made by data subjects in the EU concerning the transfer of personal data from the EU to the UK.

3 RULES APPLYING TO THE PROCESSING OF PERSONAL DATA BY COMPETENT AUTHORITIES FOR THE CRIMINAL LAW ENFORCEMENT PURPOSES

3.1 Material scope

29. In relation to recitals 24 and following of the draft decision, the EDPB notes that the draft adequacy decision does not contain much details on the activities and legal framework applicable to agencies other than the police having law enforcement duties.

30. For example, the UK Explanatory Framework for Adequacy Discussions, Section F: Law Enforcement[22], suggests on page 11 that **the National Crime Agency** (hereinafter "NCA") could be a law enforcement

[19] See Article 4 of the draft decision. See also recital 172 of the draft decision.
[20] See section 6(3) to (6) EU (Withdrawal) Act 2018.
[21] See Article 36(4) LED.
[22] See UK Government, Explanatory Framework for Adequacy Discussions, Section F: Law Enforcement, 13 March 2020.

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[23]. 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[24].

31. 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[25]. 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.

32. **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 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.**

3.2 Safeguards, rights and obligations

3.2.1 Processing on the basis of "consent" of the data subject

33. The EDPB takes note that the European Commission asserts in recitals 37 and 38 of the draft decision that **the reliance on consent** is not considered 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.

---

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf.

[23] 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.

[24] 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."

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

34. In this regard, the EDPB recalls, that Article 36(2)a) LED 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*".

35. Consent in the law enforcement context can be relevant as a legal basis for data processing, as an additional safeguard, or more generally as a basis to execute investigative powers that lead to the acquisition of personal data, for example the consent of a third party to search their premises, or to confiscate data storage.

36. The EDPB notes, based also on the information provided by the European Commission in recital 38 of the draft decision, that the use of consent, as framed in the UK regime, 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.

37. **The EDPB invites the European Commission to analyse, as a rule, the possible use of consent in a law enforcement context when assessing the adequacy of a third country under the LED.**

3.2.2 Individual rights

3.2.2.1 National security certificates

38. According to section 79 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 limitations of obligations and rights enshrined in Chapters 3 and 4 of Part 3 DPA 2018 are a necessary and proportionate measure for the protection of national security.

39. 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 restrictions but instead are a measure of transparency[26].

40. 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. 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.[27] 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 of the fact 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.[28]

41. **For the sake of comprehensiveness, the EDPB invites the European Commission to clarify in its draft adequacy decision that national security certificates can still be issued under the Data Protection Act**

[26] See UK Home Office, The Data Protection Act 2018, National Security Certificates Guidance, August 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf, p. 4.
[27] See UK Home Office, The Data Protection Act 2018, National Security Certificates Guidance, August 2020, p. 5.
[28] See UK Home Office, The Data Protection Act 2018, National Security Certificates Guidance, August 2020, p. 5.

1998. Moreover, the EDPB invites the European Commission to describe in its draft adequacy 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 adequacy decision the number of existing certificates issued under the Data Protection Act 1998, and to attentively monitor this aspect.

3.2.2.2 LED Automated decision-making

42. The EDPB stresses that Article 11(3) LED prohibits profiling that results in discrimination against natural persons on the basis of special categories of personal data. However, the EDPB notes that section 50 DPA 2018, which sets out the specific rules for automated decision making, foresees no such prohibition.

43. **The EDPB, therefore, invites the European Commission to verify this point, and explicitly state its findings in its adequacy decision. Moreover, the EDPB invites the European Commission to closely monitor cases related to automated decision making and profiling.**

44. According to the LED Adequacy Referential, *"[t]he third country law should, in any case, provide for necessary safeguards for the data subject's rights and freedoms. In this regard, the existence of a mechanism to inform the relevant Member State's competent authorities of any further processing such as the use of the transferred data for large scale profiling, should also be taken into account*"[29].

45. **The EDPB invites the Commission to assess this element in light of the guidance given by the EDPB in its referential.**

3.2.3 Onward transfers

46. According to the LED Adequacy Referential, onward transfers of personal data by the initial recipient to another third country or international organisation must not undermine the level of protection, provided for in the Union, of natural persons whose data is transferred. Therefore, such onward data transfers should be permitted only where the continuity of the level of protection afforded under EU law is ensured. The EDPB considers that, as pointed out by the European Commission in its assessment, the provisions under Chapter 5 of Part 3 DPA 2018, and in particular section 73, do in principle provide for a level of protection that is essentially equivalent to the one guaranteed under EU law, when it comes to transfer of personal data from a UK law enforcement authority to a third country.

47. First, section 73(1)(b) DPA 2018 notably provides that a controller may not transfer personal data to a third country or to an international organisation unless "*in a case where the personal data was originally transmitted or otherwise made available to the controller or another competent authority by a member State other than the United Kingdom, that member State, or any person based in that member State which is a competent authority for the purposes of the Law Enforcement Directive, has authorised the transfer in accordance with the law of the member State*." Such provisions appear to be in line with the LED Adequacy Referential, which provides that the existence of a mechanism for the relevant Member State's competent authorities to be informed and authorise such onward transfer of data has also to be taken into account. The initial recipient of the data transferred from the EU should be liable and be able to prove that the relevant competent authority of the Member State has authorised the onward transfer, and that appropriate safeguards are provided for onward transfers of data in the absence of an adequacy decision concerning the third country to which the data would be

[29] See EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, paras 59-61.

onward transferred. "*In this context, the existence of an obligation or a commitment to implement relevant handling codes defined by the transferring Member States' authorities should be taken into account*"[30].

48. **The EDPB invites the Commission to assess this element in light of the guidance given by the EDPB in its LED Adequacy Referential.**

49. Second, as explained in recital 81 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[31]. 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 36(2)(a)-(c) LED, interpreted together with recital 67 LED and the retained EU case-law. This means that, when assessing the 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 DPA 2018, 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 EU, 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[32] 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[33].

50. **The EDPB therefore 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 LED by the EU.**

51. Where the European Commission would find that no essentially equivalent level of protection to that guaranteed within the EU, as per Article 36 LED, is ensured by the 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 EU, and/or to consider the suspension of the UK adequacy decision, where personal data transferred from the EU to the UK are subject to onward transfers to the third country in question on the basis of a UK adequacy regulation**.

[30] See EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, paras 55 and 56.
[31] 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/.
[32] See CJEU, C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd and Maximilian Schrems*, 16 July 2020, ECLI:EU:C:2020:559 (hereinafter "*Schrems II*").
[33] See section 6(3) to (6) of the EU (Withdrawal) Act 2018.

52. **Finally, in relation to the international agreements concluded, or to be concluded in the future, by the UK and the possible access, by authorities from third country(ies) party(ies) to such agreements, to personal data from the EU, the EDPB recommends that the European Commission examines the interplay between the UK data protection framework and its international commitments, 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 EU 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 international agreements between the UK and third countries that risk to undermine the level of protection of personal data provided for in the EU**. For example, while the European Commission has referred to the fact that the UK-US CLOUD Act Agreement[34] may affect onward transfers to the US from service providers in the UK, **the EDPB highlights that the entry into force of this agreement may also affect onward transfers from law enforcement authorities in the UK, in particular in relation to the issuance and transmission of orders as per Article 5 of the UK-US CLOUD Act Agreement.**

53. The EDPB also considers that the conclusion of future 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 onward sharing of the information collected, since such agreements may affect the UK data protection legal framework as assessed.

54. **The EDPB therefore recommends that the European Commission continuously monitor whether the conclusion of future agreements between the UK and third countries may affect the application of UK data protection law, and provide for further limitation or exemption in relation to the onward sharing and 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 review of the level of protection afforded by the UK legislative framework and practices in relation to overseas disclosure.**

55. Finally, the EDPB takes note that in accordance with section 76(4)(b) DPA 2018 (Transfers on the basis of special circumstances), law enforcement authorities in the UK may transfer personal data to a third country or an international organisation when the transfer "*is necessary for the purpose of obtaining legal advice in relation to any of the law enforcement purposes*". **The EPDB stresses that Article 38 LED does not contain a corresponding provision; therefore invites the European Commission to clarify what is meant by legal advice, and what kind of personal data is exchanged in such cases.**

3.2.4 Further processing, including onward sharing for national security purposes

56. In its LED Adequacy Referential, the EDPB had pointed out that, concerning further processing or disclosure of data transferred from the EU for other purposes than law enforcement purposes, such as national security purposes, it should also be provided by law, be necessary and proportionate. As assessed by the European Commission in its draft decision, section 36(3) DPA 2018, the Digital Economy Act 2017, the Crime and Courts Act 2013, and the Serious Crime Act 2017 do provide for a clear legal framework allowing for onward sharing, providing that such onward sharing should be in compliance with the rules sets in the DPA 2018.

57. The EDPB notes that, in the context of further processing for other purposes of personal data transferred from the EU, the European Commission has not assessed whether there are any

[34] 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.

mechanisms for the UK law enforcement authorities to inform the relevant Member States' competent authorities of a possible further processing of data. However, the LED Adequacy Referential considers this as an element which has to be taken into account[35]. In addition, the existence of such mechanism to inform the relevant Member States' competent authorities of further processing of data for law enforcement purposes is also considered as an element to be taken into account under the LED Adequacy Referential[36].

58. **The EDPB thus invites the European Commission to complement its analysis with information about the existence of mechanisms for the UK law enforcement authorities to notify the relevant Member States' competent authorities of a possible further processing of data, transferred from the EU.**

59. Furthermore, with respect to the sharing of data collected by a criminal law enforcement authority with an intelligence agency for purposes of national security, the legal basis authorising such onward sharing is the Counter-terrorism Act 2008. In this regard, the EDPB notes that the scope and provisions of section 19 Counter-terrorism Act 2008 are not fully addressed in the European Commission's assessment, and may imply further use of a more broader nature, in particular as regards section 19(2) Counter-terrorism Act 2008, which provides that "*[i]information 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*." In this regard, the EDPB underlines that when further processed or disclosed, the data should benefit from the same level of protection as when they were processed initially by the receiving competent authority.

3.3 Oversight and enforcement

60. 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 mentions the Investigatory Powers Commissioner (hereinafter "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 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.

61. In addition, the IPC is also competent to the *ex-post* oversight of surveillance measures. It appears, however, that in this function the IPC's role is 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.

62. 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.

63. **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**

[35] See EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, para 41 and footnote 39.
[36] See EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, para 40.

to assess the independence of the Commissioner for the Retention and Use of Biometric Material, and as of the Surveillance Camera Commissioner.