

Anu Talus Chair of the European Data Protection Board

Mr Michael McGrath European Commissioner for Justice

Brussels, 5 December 2024

Via Ares

Subject: EDPB letter to the European Commission on its review of its eleven adequacy decisions adopted under Directive 95/46/EC

Dear Commissioner McGrath,

On 15 January 2024, the European Commission concluded its review of eleven existing adequacy decisions adopted on the basis of Article 25(6) of Directive 95/46/EC which remained in force by virtue of Article 45(9) of the GDPR. In its report¹, the Commission found that personal data transferred from the European Union² to Andorra, Argentina, Canada, Faroe Islands, Guernsey, the Isle of Man, Israel, Jersey, New Zealand, Switzerland, and Uruguay continues to benefit from adequate data protection safeguards. As a result, personal data transfers from the Union to these countries or territories can take place without additional requirements.

In its report, the Commission considered the data protection frameworks in the aforementioned eleven countries and territories, including the rules governing access to personal data by public authorities, in particular for law enforcement and national security purposes. The report is accompanied by a Staff Working Document (SWD)³, which presents the detailed findings of the Commission that lead to the conclusion that each of the eleven countries and territories continues to ensure an adequate level of protection for the personal data transferred from the Union.

The EDPB acknowledges the extensive work carried out by the Commission in reviewing the legislation and practices of the eleven countries and territories involved and notes that the draft report, together with the SWD, provides transparency with regards to the Commission's assessment. The EDPB also welcomes the fact that, according to the Commission's report, many countries and territories have

¹ <u>Report</u> from the Commission to the European Parliament and the Council on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC.

² Following its incorporation in the European Economic Area (EEA) Agreement, the GDPR also applies to Norway, Iceland and Liechtenstein. References to the EU in this letter are to be understood to also cover the EEA States.

³ <u>Commission Staff Working Document</u> - Country reports on the functioning of the adequacy decisions adopted under Directive 95/46/EC.

¹⁰⁴⁷ Brussels



strengthened their data protection frameworks⁴. This has led to further convergence with the EU legal framework.

As no adequacy decision was repealed, amended or suspended by the Commission, the EDPB did not provide an opinion as per Article 70(1)(s) of the GDPR, neither for the part related to the data protection framework nor for the part related to access to personal data by public authorities, which was assessed for the first time. Nonetheless, given the EDPB's involvement in previous reviews of adequacy decisions⁵ and its experience in this field⁶, the EDPB, while not questioning the substance of the report, would like to provide the Commission with observations on the methodology of its adequacy assessment and certain aspects that could have been described in more detail in the report and the SWD. The EDPB believes these aspects deserve close monitoring by the Commission in its future re-evaluations of third countries and territories' laws and practices under Article 45(4) GDPR and Article 97(2)(a) GDPR.

I. General remark

In line with Article 45(2)(a) and Recital 104 of the GDPR, the Commission's assessment of a third country takes into account how a particular third country respects the rule of law, access to justice as well as international human rights norms and standards. In light of this and in view of current developments, the EDPB would like to seize this opportunity to invite the Commission to provide more transparent information on the assessment of these elements, in law and in practice, in the context of future adequacy decisions and reviews.

II. Observations on the methodology of the assessment of the data protection framework

When carrying out the adequacy reviews, according to Article 45(4) GDPR, the European Commission shall focus on the relevant developments in the legal frameworks of the third country or international organisation. The EDPB notes that accordingly, the January 2024 report and its SWD related to the eleven adequate third countries and territories did not provide a full description of the laws and practices of each third country or territory.

⁴ <u>Report</u> from the Commission to the European Parliament and the Council on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC, pages 5-6.

⁵ See, in this regard, the EDPB considerations included in the <u>Adequacy Referential</u> (issued by the Article 29 Working Party and adopted on 28 November 2017, WP 254) according to which, in order to allow the EDPB to provide the European Commission with an opinion on whether the third country, a territory or one or more specified sectors in this third country or an international organization, no longer ensures an adequate level of protection, the EDPB should be kept informed of any review process and review mission in the third country or to the international organization and would also appreciate to be invited to participate in these review processes and missions. See also, on this, Article 97(4) and Recital 106 GDPR according to which, for the purposes of carrying out the periodic reviews of the adequacy decisions envisaged by Article 97(2)(a) GDPR, the Commission should take into consideration, along with the views and findings of the European Parliament and of the Council, also the views of other relevant bodies.

⁶ Article 29 Working Party (Art. 29 WP) had issued opinions on each one of the adequacy decisions adopted under Directive 95/46/EC at the time of their adoption. They can be found <u>here.</u>

European Data Protection Board

Rue Wiertz, 60 1047 Brussels



However, these adequacy decisions were adopted several years ago⁷ and the elements to be taken into account in an adequacy assessment have evolved since the adoption of the original adequacy decisions⁸. Against this background, the EDPB would have found it useful if this report contained a more comprehensive description of the elements of the adequacy assessment for each country and territory. The EDPB would also suggest, for future reports on the re-evaluation of the data protection frameworks related to these eleven adequate third countries and territories, that they contain a detailed description of the elements of the adequacy assessment for each country and territory or at least include references to previous reports or adequacy decisions where those elements are referred to.

In this perspective, the EDPB considers that such future adequacy review reports could state more clearly which aspects of the third country laws and practices have been checked and have remained unchanged (and are not described in the report for this reason), as well as which aspects have evolved since the adoption of the initial decisions. This would provide a more comprehensive overview on the data protection guarantees existing in the assessed jurisdictions and might contribute to positive developments of the legal framework in other third countries. Additionally, it would provide data subjects with more transparency and enhance their understanding with regards to exercising their rights in the third country.

In particular, in this regard, the EDPB would like to draw the Commission's attention to the following aspects that are not mentioned consistently in the reports of *all* eleven countries and territories.

The EDPB would therefore suggest describing in more detail in their future adequacy reviews for these eleven countries and territories:

- the legal notions of "controller", "processor" and "recipient" or of equivalent notions⁹; Although these data protection concepts do not have to mirror the GDPR terminology, they should reflect and be consistent with the concepts enshrined in European data protection law¹⁰;
- ii. **the legal bases under which personal data may be lawfully, fairly and legitimately processed**; The Union framework acknowledges several legitimate grounds for data processing including, but not limited to, performance of a contract or the legitimate interests of the controller or a third party which do not override the interests of the individual¹¹; The

⁷ The decisions on New Zealand and Uruguay were adopted in 2012, that of Canada was adopted in 2001 and that of Switzerland was adopted in 2000.

⁸ See Judgment of the Court of Justice of the EU of 6 October 2015 in Case C-362/14, Maximillian Schrems v Data Protection Commissioner (<u>Schrems I</u>), ECLI:EU:C:2015:650; Judgment of the Court of Justice of the EU of 16 July 2020 in Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd. and Maximilian Schrems (<u>Schrems II</u>), ECLI:EU:C:2020:559. ; See Adequacy Referential.

⁹ This issue is not expressly described in the reports of Andorra, Canada, Israel and New Zealand. It is on the contrary mentioned in the cases of Argentina, Faroe Islands, Guernsey, Isle of Man, Jersey, Switzerland and Uruguay, where such definitions exist.

¹⁰ EDPB <u>Opinion 28/2018</u>, §63-66; <u>Opinion 32/2021</u>, §45 and 54; <u>Opinion 5/2023</u>, §40.

¹¹ Opinion 32/2021, §63.

European Data Protection Board

Rue Wiertz, 60 1047 Brussels



EDPB considers that the existence of legal grounds other than consent¹² (since consent has been sufficiently outlined in the reports) should be described in more detail in future assessments.

- iii. the fact that individuals in the EU can exercise their rights in the third countries and territories, as this would provide more transparency especially vis-à-vis data subjects;
- iv. the inclusion of general descriptions and reassurances on limitations applicable to data subjects' rights¹³ and not only in the context of access to the transferred data by third country authorities; In this regard, the EDPB recalls that restrictions to data subject's rights should respect the essence of the fundamental rights and freedoms, and should be necessary and proportionate in a democratic society¹⁴;
- v. the safeguards related to automated decision-making¹⁵, including the right to be informed about the specific reasons underlying the decision and the logic involved, to correct inaccurate or incomplete information, and to contest the decision where it has been adopted on an incorrect factual basis¹⁶, which the EDPB considers particularly important against the backdrop of the exponential development of AI technologies¹⁷.
- vi. the international commitments the third country has entered into¹⁸ 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. Adherence to international human rights commitments, to binding and non-binding international commitments are an indication of the respect of fundamental rights of individuals, including the right to the protection of personal data¹⁹;
- vii. the **rules on onward transfers** in the assessed third countries and how their application in practice²⁰ has developed since the adoption of the adequacy decisions. The EDPB notes in this regard that the applicable legal frameworks in particular, in what concerns the transfer mechanisms available appear to be, in some cases, very different from the ones set out under EU law, and recalls that the level of protection of individuals whose personal data is

European Data Protection Board

Rue Wiertz, 60 1047 Brussels

¹² This issue is not mentioned in the reports of Jersey, Israel and Uruguay. It is on the contrary mentioned in the cases of Andorra, Argentina Canada, Faroe Islands, Ile of Man, New Zealand (partially) and Switzerland.

¹³ This aspect is not mentioned in the reports of Argentina, Canada, Israel and Uruguay. It is on the contrary mentioned in the cases of Andorra, Faroe Islands, Guernsey, Isle of Man, Jersey, New Zealand, Switzerland.

¹⁴ See Adequacy Referential, Chapter 2.A.8; See also Opinion 28/2018, §93 and 95.

¹⁵ See Adequacy Referential, Chapter 3.B.3.

¹⁶ This aspect is not mentioned in the reports of Argentina Canada, Israel and New Zealand. It is on the contrary mentioned in the cases of Andorra, Faroe Islands, Guernsey, Isle of Man, Jersey, Switzerland and Uruguay.

¹⁷ See also Opinion 5/2023, §62-65.

¹⁸ This aspect is not mentioned in the reports of Canada, Israel and New Zealand. It is on the contrary mentioned in the cases of Andorra, Argentina, Faroe Islands, Guernsey, Isle of Man, Jersey, Switzerland and Uruguay.

¹⁹ See Recital 105 of the GDPR; Article 45(2)(c) GDPR; Adequacy Referential, Chapter 1 & Chapter 3.C.2 and 4; Opinion 32/2021, §34; Opinion 28/2018, §57; Opinion 5/2023, §22.

²⁰ For example, a description of the specific safeguards to be implemented by the exporter and their functioning, if possible with references to guidelines adopted by the competent data protection authority in this regard.



transferred to a third country must not be undermined by onward transfers to other third countries²¹.

III. Observations applying to the access to and use of personal data transferred from the EU by public authorities in the third countries.

Government access to personal data by third country public authorities gained genuine significance for the question of whether a third country provides an adequate level of protection following the findings of the Court of Justice of the European Union (CJEU) in its *Schrems I* judgement²². The CJEU finds that data collection and processing by public authorities, in particular for law enforcement and national security purposes, is a key element of the adequacy standard²³. The GDPR reflects this by explicitly referring in Article 45(2)(a) to legislation concerning public security, defence, national security, criminal law and the access of public authorities to personal data.

Against this background, government access to personal data has not been examined by the Commission in the procedure for adopting the eleven adequacy decisions now confirmed in its report, as the latter were still adopted under the former EU data protection framework and pre-date the CJEU's jurisprudence mentioned above. The EDPB therefore welcomes that the report of the Commission now provides an assessment of the legal framework governing the access to and use of personal data transferred from the EU by public authorities of the third countries that were found to provide an adequate level of protection pursuant to Article 25(6) of the Directive.

At the same time, the EDPB notes that the information provided in the SWD is not as detailed as in the context of a draft adequacy decision submitted to the EDPB for its opinion as per Article 70(1)(s) GDPR. In addition, as mentioned above, the EDPB was not formally consulted by the Commission since no adequacy decision was repealed, amended or suspended. It is therefore within these limits, and on the basis of the standard elaborated for surveillance measures framed as the "European Essential Guarantees"²⁴, that the EDPB wishes to address its following observations on government access for law enforcement and national security purposes which require particular attention and monitoring in the future.

National legal systems may provide for exemptions from the applicable data protection rules for law enforcement and national security purposes, typically on grounds of prejudice to legitimate public interests and objectives, such as the prevention, detection or investigation of a crime. Exempted provisions may include, for example, rules relating to the general principles of data processing, data subject rights as well as oversight functions and powers. The EDPB would like to emphasise that such exemptions and limitations need to be applied restrictively to ensure that they

²¹ Adequacy Referential, Chapter 3.A.9.

²² See note 7 above.

²³ Ibid, §84 et seq. The Court clarified that the Commission's assessment should not be limited to the general data protection framework of the third country but should also include the legal framework for government access to personal data.

²⁴ <u>EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures</u>, adopted on 10 November 2020.



are only invoked to the extent necessary and proportionate in a democratic society. It should not be possible to rely on exemptions from data protection standards in a blanket manner. In cases of exemptions on grounds of prejudice, competent authorities should be able to demonstrate that there is a real possibility of an adverse effect on the protected public interest *if* the relevant provision would

be applied without restriction. Additionally, they should take into account the need for regular review of the circumstances justifying such limitations and for restoring their application where the justification for the limitations ceases to exist. The EDPB invites the Commission to monitor the application of aforementioned exemptions in practice, in particular in jurisdictions where the law is broadly drafted and framed through interpretative but non-binding guidance issued by supervisory authorities. The Commission should follow up in future reports on the compliance with such guidance by governmental bodies.

Following additional explanations provided by the Commission, the EDPB notes that the Commission has undertaken an **analysis of the impact of more general exceptions on the right to privacy and the protection of personal data for its reports (e.g. states of emergency).** However, in particular from the point of view of access to personal data by public authorities, the EDPB would have appreciated if the Commission had included this analysis or at least its impact on the adequacy findings in the SWD, and thus made it publicly available.

Moreover, the EDPB encourages the Commission to draw up a more detailed overview of the intelligence landscape in the examined jurisdictions. The EDPB is aware that not all intelligence agencies in a given jurisdiction have access to personal data transferred or being transferred from the Union and that the methodology for drafting these reports depend on the information provided by the states under review. The EDPB believes that such an overview would strengthen the data subjects' understanding of the rights and the remedies available to them and, thereby, put them in a better position to exercise their rights.

Particularly in the area of government access for law enforcement and national security purposes, oversight processes are likely to be multi-layered, involving several oversight structures, with differing powers. For example, supervisory authorities may have extensive investigatory powers, but may not have binding remedial powers. In light of this, the EDPB invites the Commission to closely monitor to avoid that there is a gap between responsibilities and competences allocated to different oversight bodies in national systems. The EDPB encourages the Commission to ensure that supervisory authorities collectively have adequate enforcement powers to ensure compliance with data protection laws.

Another area for particular attention is represented by the **national provisions allowing, under certain conditions, business organisations or public sector bodies to disclose personal information on a voluntary basis** (i.e. upon informal requests from law enforcement authorities and intelligence

European Data Protection Board Rue Wiertz, 60 1047 Brussels



agencies or on their own initiative). In this regard, it is essential that appropriate safeguards are envisaged to protect the rights and interests of the concerned individuals against arbitrariness²⁵.

Moreover, with regard to ex-post reviews, the obligation to keep record of voluntary disclosures is essential since it allows oversight bodies to conduct full reviews of the use of these measures (e.g. with regard to the decision to disclose and the reasons to disclose as well as the information disclosed). Therefore, the EDPB invites the Commission to closely monitor the national provisions allowing law enforcement authorities and intelligence agencies to obtain personal data transferred under the adequacy decisions through voluntary disclosures and their application in practice as well as the developments in the relevant legal framework.

The EDPB stands ready to be involved in the next periodic review of the eleven adequacy decisions adopted under the Directive 95/46/EC, as the EDPB does for all the periodic reviews of adequacy decisions adopted under the GDPR.

Yours sincerely,

Anu Talus

Cc : Ms. Ana Gallego Torres, Director-General (DG JUST)

²⁵ Such as an effective prior assessment or ex-post review by independent oversight bodies regarding the legality, necessity and proportionality of informal requests or proactive decisions to disclose, the adoption of adequate measures to mitigate the impact on the fundamental rights and freedoms of data subjects, as well as the obligation to consider the reasonable expectations of the concerned individuals and the adoption of less intrusive means to access personal information.