EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS

Unit .01 – International Affairs and Data Flows

Brussels, 26 April 2024
JUST.01

Subject: Your letter of 6 September 2023 (ref.: Ares((2023)6307380))

Dear Sir/Madam,

Thank you for your letter of 6 September to Commission President von der Leyen regarding the adequacy decision on the EU-U.S. Data Privacy Framework, which was adopted by the European Commission on 10 July. The President asked me to reply on her behalf.

The adequacy decision([1]) is based on a detailed assessment of the U.S. legal framework, including the limitations and safeguards that apply when personal data transferred from the EU to the U.S. is accessed by U.S. national security agencies. This includes in particular the Executive Order on 'Enhancing Safeguards for United States Signals Intelligence Activities', which was adopted by the U.S. President as a result of negotiations between the European Commission and the U.S. government([2]). This Order introduced significant changes to the US legal framework in order to address the points raised by the Court of Justice of the European Union in its *Schrems II* decision as regards the previous transatlantic data transfer arrangement (the Privacy Shield) ([3]).

In particular, new binding and enforceable safeguards have been introduced in U.S. law to ensure that the collection and use of personal data of foreigners (including Europeans) by U.S. intelligence agencies is limited to what is necessary and proportionate in pursuit of defined national security objectives. In this context, it is important to note that the Executive Order does not just refer (in the abstract) to general notions of necessity and proportionality, but further specifies these terms through concrete requirements ([4]). For

([1]) Commission Implementing Decision EU 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, C(2023)4745 ('Adequacy decision on the EU-US Data Privacy Framework'). Available here : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023D1795&qid=1696318804711.

([2]) On those negotiations, see for instance https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_1443 and https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087.

([3]) Case C-311/18 of 16 July 2020, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems.

([4]) See also Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework (https://edpb.europa.eu/system/files/2023-02/edpb_opinion52023_eu-us_dpf_en.pdf), page 4 of the

example, the Executive Order lists the factors that intelligence agencies must take into account and balance in deciding whether and how to conduct surveillance. These include the same factors as the ones required by the case law of our Court of Justice (and the European Court of Human Rights), such as the importance of the public interest pursued, the impact on the privacy of individuals and the intrusiveness of the specific measure to be used. In other words, the necessity and proportionality requirements are not only expressly defined in the Executive Order but they are defined in a similar way than under EU law, as interpreted by the European Court of Justice.

Moreover, the limitations and safeguards introduced by the Executive Order supplement those provided by Section 702 FISA and EO 12333. This means that the new requirements of the Executive Order must be applied by intelligence agencies when engaging in signals intelligence activities both within the United States (on the basis of FISA) and while data is in transit to the United States (on the basis of EO 12333) ([5]).

Regarding your comment on mass surveillance, it is first of all important to note that the Executive Order only allows the collection of data in bulk, i.e. the collection of larger volumes of data without targeting specific individuals or specific communication facilities (e.g., an email address), not the generalised and indiscriminate collection of data ("mass surveillance"). Whereas general and indiscriminate surveillance is clearly illegal, bulk collection, in itself, is not ([6]). Moreover, the collection of data in bulk under the Executive Order is only allowed outside the US (on the basis of EO 12333) and is framed through appropriate limitations, conditions and safeguards ([7]). In particular, in addition to the general limitations and safeguards on legality, necessity, and proportionality ([8]), the specific safeguards for the collection of data in bulk apply ([9]). For example, the Executive Order requires that targeted collection must be prioritized and bulk collection may only take place when a specific objective (e.g., the fight against terrorism) cannot be achieved through targeted collection. If bulk collection is nevertheless used by US intelligence agencies, measures (including technical measures) must be applied to limit as much as possible the data collected (and thus by minimising non-pertinent information). Finally, there are different oversight mechanisms in place in the US that supervise the use of bulk collection ([10]) and effective independent review is provided by the Data Protection Review Court, in response to complaints from individuals.

Moreover, a new redress mechanism has been created, which includes the independent and impartial Data Protection Review Court (DPRC) to investigate and resolve complaints of EU individuals regarding the collection and use of their data by U.S. intelligence agencies ([11]).This redress mechanism is accessible to any EU individual, who can lodge a complaint free of charge and without having to demonstrate that data was in fact accessed

---

Executive Summary and paras. 125-126. The EDPB recognised in its opinion that the EO introduces in US law requirements reflecting the principles necessity and proportionality foreseen under EU law and in the CJEU and ECHR case-law.

([5]) See adequacy decision on the EU-US Data Privacy Framework recital 125.

([6]) See CJEU C-311/18, *Facebook Ireland et Schrems (Schrems II)*, EU:C:2020:559, paragraph 183; ECtHR, *Centrum för rättvisa c. Suède*,no. 35252/08, § 261.

([7]) Adequacy decision on the EU-US Data Privacy Framework recital 141.

([8]) See adequacy decision on the EU-US Data Privacy Framework recitals 127-132.

([9]) See adequacy decision on the EU-US Data Privacy Framework recital 141.

([10]) Adequacy decision on the EU-US Data Privacy Framework recitals 161-174.

([11]) See adequacy decision on the EU-US Data Privacy Framework recitals 184-194.

or that any harm was suffered. Individuals can submit complaints in one of the official EU languages to the national data protection authority, which will ensure that the complaint will be properly transmitted to and resolved by the new redress mechanism in the US ([12]).

To ensure that such complaints are handled by an independent redress mechanism the Executive Order provides a number of guarantees. In particular, the DPRC is composed of members from outside the US Government, who are appointed on the basis of specific qualifications, can only be dismissed for cause (i.e. misconduct, malfeasance, breach of security, neglect of duty or incapacity) and cannot receive instructions from the government([13]). Moreover, the DPRC has the powers to investigate complaints from EU individuals (e.g. by obtaining relevant information from intelligence agencies, including classified information) and is equipped with binding adjudicative and remedial powers (e.g. this may include, for instance, to order the deletion of any data that was collected in violation of the safeguards provided in the Executive Order). In each case, the Court will select a special advocate with relevant experience to support the Court, who will ensure that the complainant's interests are represented and that the Court is well informed of the factual and legal aspects of the case ([14]). This ensures that both sides are represented and introduces important guarantees in terms of fair trial and due process. When the procedure before the DPRC is completed, the complainant will be informed that either no violation of US law was identified, or that a violation was found and remedied. The US Department of Commerce is required to maintain a record for each complainant who submitted a complaint and give access to the full reasoned decision once it no longer poses a risk for national security ([15]). Finally, the correct functioning of this redress mechanism will be subject to regular and independent evaluations. As part of the review, the Privacy and Civil Liberties Oversight Board (an independent body) will, for example, assess whether complaints are handled in a timely manner; whether the DPRC has full access to the necessary information; whether the DPRC decisions are complied with by the intelligence community and whether and how the DPRC applies the safeguards provided for in the Executive Order ([16]).

Finally, as with any other adequacy decision, the Commission will continuously monitor relevant developments in the United States and regularly review the adequacy decision. The first review will take place within one year after the entry into force of the adequacy decision, to verify whether all relevant elements of the US legal framework are functioning effectively in practice ([17]).

([12]) See adequacy decision on the EU-US Data Privacy Framework recital 177.

([13]) See Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework para 229, where the EDPB recognised that these guarantees provided for by the Executive Order "*do not give reason to doubt the DPRC's independence*".

([14]) See adequacy decision on the EU-US Data Privacy Framework recital 188.

([15]) See adequacy decision on the EU-US Data Privacy Framework recital 193.

([16]) See adequacy decision on the EU-US Data Privacy Framework recital 194.

([17]) See adequacy decision on the EU-US Data Privacy Framework recitals 208-214.

Against this background, we consider that the adequacy decision on the EU-US Data Privacy Framework provides for effective protection of EU citizens' data and legal certainty and stability for transatlantic data flows.

I hope you find the above clarifications helpful.

Yours sincerely,

Bruno GENCARELLI
Head of Unit