PISM | POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

NO. 101 (2220), 27 JULY 2023 © PISM

BULLETIN

Three Times Lucky?
EC Decides on New Rules for EU-U.S. Data Flows

Stefania Kolarz

In its Decision of 10 July, the European Commission (EC) confirmed that it considers the newly agreed level of personal-data protection in the U.S. meets EU standards. While this will facilitate cooperation between European and American companies, it may prove to be a short-term solution. The European Data Protection Board (EDPB), activists, and others have already pointed out imperfections in the U.S. data protection system. Potential court complaints based on their arguments may lead to the annulment by the Court of Justice of the EU (CJEU) of another EC Decision simplifying the transfer of personal data to the U.S., following the strikes to the Safe Harbor and Privacy Shield Decisions.

Transfers of Data to Third Countries. The EU Data Protection Regulation (GDPR), applicable in the EU as well as Iceland, Liechtenstein, and Norway, provides strict conditions for the lawful transfer of data to third countries. The receiving country must be shown to provide rights and remedies comparable to the GDPR. The surest confirmation of such status is a Decision by the European Commission (EC) establishing the existence of an adequate level of protection that aligns with the rules for data transfers to a third country with those applied in the EU. However, such Decisions are few in number, so far obtained by Israel, Japan, the UK, and some additional states. In other cases, data transfers are possible but subject to additional actions and carry a higher risk of breaching the GDPR. These transfers can be based on, among others, standard contractual clauses (SCCs) or, for companies operating in several countries, binding corporate rules (BCRs), as well as after conducting a third-country data-transfer-impact assessment (TIA). As SCCs are implemented by companies individually, they often differ from the model proposed by the EC and are subject to time-consuming review and a TIA. An additional disadvantage of this method is possible discrepancies in the assessment of the quality of protection by the transferring company and the data protection authority to which data subjects can file complaints. BCRs, on the other hand, must be approved in advance at the national level and then by the EDPB, which can be cumbersome for companies.

The issue of legality also arises when transferring data to the United States. In 2000, the U.S. obtained a decision from the EC (Safe Harbor), but whistleblower Edward Snowden's revelations of extensive access by U.S. security services to Europeans' data raised concerns about the impact of the transfers. These were used in cases brought against Facebook by the activist Max Schrems. As a result of these cases, in 2015 the CJEU annulled Safe Harbor, and in 2020 another cooperation framework, first introduced in 2016, called Privacy Shield, replaced it. Schrems also showed that, among other things, the U.S. does not provide a way for Europeans to challenge how their data are processed, and the CJEU found that U.S. law gives the authorities access to data disproportionate to the goal of ensuring national security. This has forced U.S. companies to use other solutions, such as SCCs or BCRs or to move or open subsidiaries in the EU (to limit data transfers to the U.S.), and in some cases to abandon cooperation between European and U.S. companies. For example, Facebook's parent company Meta has no plans to introduce Threads (its Twitter equivalent) to the European market, and when the Irish data authority invalidated Meta's SCC in May this year, the company hinted that it might withdraw its social networking sites Facebook and Instagram from Europe.

New Rules. Following a second ruling connected to Schrems' assertions, the EC and the U.S. Department of Commerce entered into negotiations on the issues raised by the CJEU that culminated in March last year in a preliminary agreement on a new EU-U.S. Data Privacy Framework (DPF). As a result, in autumn 2022, President Joe Biden signed an executive order that restricted the processing of personal data for intelligence purposes. It is now only permitted for a pre-defined national security purpose, in a proportionate manner and respecting the private life of the data subject. Meanwhile, the U.S. Office of the Director of National Intelligence (ODNI) confirmed that the Intelligence Community, which comprises 18 U.S. intelligence agencies, has adopted new procedures to implement the presidential order, including strengthening controls over access to data. It has also created avenues of redress, including a Civil Liberties Protection Officer at the ODNI and a Data Protection Review Court within the Attorney General's office.

Under the DPF, individuals whose data is transferred to the U.S. have been given the right to access their data, correct it, and request the deletion of information that is incorrect or obtained in violation of the law. For U.S. companies, participation in the DPF is voluntary. Provided they commit to the principles pertaining to the framework (minimising data processing, implementing certain security measures for transfers to third countries, etc.), they will receive special certificates. Companies that had attestations issued under Privacy Shield (around 3,000) will benefit the soonest from the DPF, as it will be simpler for them to adapt to the new conditions than to implement a data protection framework from scratch. Certificates issued by the Commerce Department will allow the transfer of data from the EU without additional restrictions.

Drawbacks of the Solution. The DPF is a partial solution. Certification only applies to companies under the jurisdiction of the Federal Trade Commission or the Department of Transport, which means it excludes application to non-profit organisations, banks, and other financial institutions. The basis for transferring data from Europe to these entities therefore remains the option of an SCC or BCR, among others. However, the new framework is intended to make it easier for them to carry out TIAs because the changes introduced (including restrictions on agency access to data and redress measures) will apply to all data regardless of the basis on which it is processed.

While most Member States and the EC have approved the U.S. changes, these remedies are controversial within the Union. The EDPS views the new framework positively compared to the previous arrangements but points to remaining gaps in protection, such as the lack of specific rules for automated data processing and profiling and the subordination of appellate authorities to the U.S. executive. There are also practical concerns, including whether U.S. authorities will interpret proportionality and necessity of data processing more liberally than the EU. The European Parliament, meanwhile, is critical of the exceptions in the DPF allowing for the mass processing of Europeans' data in cases of emergencies related to climate change and health crises. Although these opinions, being non-binding, did not lead to the EC's Decision being blocked, Schrems has already announced a legal challenge to the new framework by the end of August this year. He sides with the objections raised within the EU, and additionally considers the changes insufficient to address the application of Section 702 of the U.S. Foreign Intelligence Surveillance Act, which, among other things, allows for the collection and transfer to third countries of information on foreign nationals located outside U.S. territory and considered a threat to national security. It therefore raises the risk of the U.S. transferring the personal data of Europeans to third countries applying lower standards of protection.

Conclusions and Perspectives. The DPF is an attempt to balance several values: respect for the privacy rights of Europeans, U.S. security, and the interests of EU and U.S. businesses. The EC's Decision is beneficial from the perspective of European businesses because it increases legal certainty and reduces the risk of potential allegations of violations of the GDPR when working with U.S. partners. Its positive effects will be felt especially by large technology companies, which are particularly prone to complaints from people whose data they process. The decision is also an improvement for smaller companies, which often decline to work with U.S. companies because they do not have sufficient resources to carry out TIAs and consider the risks to be disproportionate to the expected gains.

The objections to the DPF, raised in just several months, could lead to another annulment by the CJEU of the transfer of data from the EU to the U.S. under the simplified rules. Given the far-reaching concessions made by the U.S. (the EU has *de facto* brought about a change in American law, and the protection will also be applied to the data of U.S. citizens), it can be assumed that further demands by the EU will not meet with a favourable response from the U.S. Therefore, there is a risk that the only result of a potential challenge to the new framework will be, once again, to make things more difficult for businesses, in particular smaller firms, which will also be disadvantageous for Polish companies seeking to intensify their cooperation with the U.S.