BRANDI
RECHTSANWÄLTE

THIRD COUNTRY TRANSFERS - NEW ADEQUACY DECISION FOR THE U.S.

Information on data protection I September 2023

Introduction

International data transfers occur in everyday corporate life in connection with the use of a variety of online applications. This applies, for example, to the use of video conferencing services such as Microsoft Teams and Zoom, the use of applications such as Office 365, and the integration of cloud and e-mail services, but also to the cooperation and exchange of data with other Group companies. In particular, collaboration with U.S. service providers and partners remains highly relevant for a majority of companies, despite the data protection difficulties associated with international data transfers. In the survey "Data Protection in German Business: GDPR & International Data Transfers", published by the digital association Bitkom in the fall of 2022, almost two-thirds of the companies surveyed said that not transferring data internationally would have serious negative consequences for them. Responders also made clear the importance of a robust legal basis for international data transfers.

Data protection requirements for data transfers to third countries

The aim of the General Data Protection Regulation (GDPR) is to ensure an equivalent level of protection for personal data in all EU member states. According to Recital 103, the transfer of personal data from the EU to recipients in a third country or to international organizations should not fall below the level of protection provided within the EU. For this reason, international data transfers require special safeguards. Article 44 GDPR stipulates that any transfer of personal data to a third country or to an international organization is only permitted if the data controller and processor comply with the requirements and provisions laid down in the GDPR. The provisions of the fifth chapter of the GDPR (Article 44 - 50 GDPR) contain specific requirements that must be met when transferring personal data to third countries or international organizations. In particular, a data transfer may only take place if it can be ensured in advance that a level of data protection comparable to the level of data protection in the EU is guaranteed in the third country concerned. The GDPR provides for various mechanisms to ensure this.

Article 45 GDPR first regulates the transfer of data on the basis of an adequacy decision. Accordingly, a transfer of personal data to a third country may be made if the European Commission has decided that the third country, a territory or one or more specific sectors in the third country have an adequate level of protection. If an adequacy decision exists, data transfers to this state do not require special case-by-case approval. However, such decisions exist for only a few countries. A complete list of countries for which an adequacy decision currently exists can be found on the European Commission's website. If the European Commission has determined a comparable level of data protection in an adequacy decision, target companies in the respective state may be treated as if they were companies from the EU in terms of data protection law. In case of data transfers to the U.S., however, the special feature must be taken into account that only those companies that participate in the new "EU-US Data Privacy Framework" are covered by the resolution.

In the absence of such a decision and if the third country concerned does not provide an adequate level of data protection as confirmed by the European Commission, personal data may only be transferred if the data controller or processor has provided appropriate safeguards and the data subjects have enforceable rights and effective remedies.

In this respect, the conclusion of the EU standard contractual clauses comes into consideration – a contract stipulated by the European Commission between the data exporter from the EU and the data importer in a third country, in which the non-European company undertakes to comply with the requirements stipulated by the European Commission and to ensure an appropriate level of data protection.

In addition, a comparable level of data protection for companies in third countries can also be achieved through the use of Binding Corporate Rules within the meaning of Article 47 GDPR, in which companies commit themselves to comply with a minimum data protection standard, as well as through approved codes of conduct within the meaning of Article 46 (2) (e) in conjunction with Article 40 GDPR. However, these must be approved by the responsible supervisory authority before they are used.

If neither an adequacy decision nor suitable safeguards are available, international data transfer is only possible in exceptional cases. In this respect, the existence of an explicit and informed consent of the data subject may be considered, Article 49 (1) (1) (a) GDPR.

Safeguarding data transfers to the U.S. to date

While data transfers to the U.S. were in the past mostly based on the EU-US Privacy Shield, a special agreement between the EU and the U.S. that granted certified companies an adequate level of data protection, 91 % of companies now use standard contractual clauses provided by the European Commission to safeguard data transfers. The European Court of Justice (ECJ) declared the EU-US Privacy

Shield invalid in its decision "Schrems II" (ECJ, decision dated 16.07.2020 - Ref. C-311/18) in July 2020 and also imposed additional requirements with regard to the use of standard contractual clauses. In its decision, the ECJ stated that the U.S. does not have a level of data protection that corresponds to the standards within the EU and that the fundamental rights of EU citizens are not sufficiently protected; in particular, the far-reaching access powers of U.S. security authorities and the lack of effective legal remedies were problematic in the view of the ECJ.

In response to the ECJ decision, the European Commission published new adapted standard contractual clauses in June 2021, which can now be used to safeguard data transfers to third countries. The new standard contractual clauses take account of the ECJ's concerns by specifying, among other things, concrete behavioral obligations in the event of a government disclosure request (clauses 15.1 and 15.2 of the standard contractual clauses). It should be noted that the conclusion of the clauses does not, however, eliminate the data exporter's obligation to examine whether an adequate level of data protection can be guaranteed despite the transfer of data to a third country. Accordingly, a data transfer based on the standard contractual clauses is only permissible if the applicable national regulations do not counteract the obligations resulting from the standard contractual clauses. In order to meet these requirements, it is advisable to prepare a transfer impact assessment for the international transfer of data, which can also include additional safeguards.

The new adequacy decision for the U.S.

The European Commission has now adopted a new adequacy decision for the EU-US Data Privacy Framework as of July 10, 2023. It states that the United States ensures an adequate level of protection - comparable to that of the EU - for personal data transferred from the EU to U.S. companies within the new data protection framework.

In order for a data transfer to a U.S. company to be based on the adequacy decision, the company must participate in the new data protection framework and join the agreement, as was previously the case with the EU-US Privacy Shield. To join the EU-US Data Privacy Framework, companies must commit to a variety of data protection obligations, including compliance with data protection principles, data security obligations, and obligations to delete personal data and ensure the continuity of protection when the data is disclosed to third parties. The new guarantees are intended to address the concerns previously expressed by the ECJ.

In particular, the new regulations provide for stricter requirements for intelligence access to data of Europeans; access by U.S. security agencies is to be limited to a necessary and proportionate level. The activities of U.S. intelligence agencies are also to be subject to increased oversight. Furthermore, as there should be various independent and impartial redress mechanisms for EU citizens in the event of what they perceive to be unlawful access to their data, provision is made, among other things, for the creation of a Data Protection Review Court (DPRC) to which individuals in the EU can turn. Free independent dispute resolution mechanisms and an arbitration board are also provided for.

As early as spring 2022, the European Commission and the United States had reached an agreement in principle on a new transatlantic data protection framework. Joe Biden then signed a decree in October last year that creates the legal basis on the U.S. side for a new legal framework for data transfers to the U.S. (we reported in November 2022). The European Commission then submitted a draft adequacy decision for the U.S. in December 2022 and initiated the procedure for adopting the adequacy decision. Subsequently, various bodies in the EU, including the European Data Protection Board (EDPB) as well as the competent committee of the EU Parliament (LIBE), have commented on the draft (we reported in April and in May 2023). The EDPB welcomed the planned improvements on the previous regulations, but at the same time expressed criticism with regard to various points and asked the European Commission for further investigations in this respect. The EDPB's comments concerned, in particular, certain rights of data subjects, onward transfers of personal data, and the practical functioning of the redress mechanism. The LIBE Committee expressed a similar view, but took an even stronger stance, rejecting approval without an attempt at further renegotiation with the United States. It pointed out that there was still a lack of sufficient safeguards and that bulk collection of personal data was still permissible in certain cases. There was also criticism that the DPRC's decisions are secret, which, among other things, violates citizens' right to access their data.

By means of the new adequacy decision, personal data should now be able to be transferred securely to U.S. companies participating in the Data Privacy Framework without the need for additional data protection safeguards, according to the European Commission. President Ursula von der Leyen has said: "The new EU-US data protection framework will ensure secure data flows for Europeans and provide legal certainty for companies on both sides of the Atlantic. Following the agreement in principle I reached with President Biden last year, the U.S. made unprecedented commitments to create the new framework. Today, we are taking an important step forward in giving citizens confidence in the security of their data, deepening our economic relationship between the EU and the U.S., and strengthening our shared values at the same time. The framework shows that by working together, we can address the most complex issues."

The privacy framework is administered and overseen by the U.S. Department of Commerce; enforcement against certified U.S. companies is the responsibility of the U.S. Federal Trade Commission. In addition, regular reviews of the EU-US Data Privacy Framework by the European Commission, representatives of the European data protection authorities, and the competent U.S. authorities are planned in order to check whether the planned measures have been implemented and are functioning effectively. An initial review is scheduled to take place within the next year.

Effects and recommendations for action

The adequacy decision entered into force upon its adoption on July 10, 2023 and has been directly applicable since then without any further implementation steps, so that data transfers can in principle be based on the EU-US Data Privacy Framework with immediate effect. However, since the new adequacy decision only applies to companies that have committed to comply with the new data protection regulations and have joined the agreement, companies must check in advance of the data transfer for each specific case whether the U.S. company in question is certified under the EU-US Privacy Data Framework. The U.S. Department of Commerce publishes a corresponding list of certified companies that can be used for the audit. The major IT groups such as Microsoft, Google, Meta and Amazon have already committed to compliance and joined the agreement, while Apple is not yet on the list.

On the one hand, the new adequacy decision makes it easier to secure data transfers to the U.S. again, but on the other hand it does

not automatically eliminate the critical points that have been raised, for example, with regard to the use of Office 365. It cannot be assumed that the EU-US Data Privacy Framework will lead to more legal certainty - at least from a technical point of view - as data transfers will not become immediately more secure despite the envisaged improvements. In view of the massive criticism voiced by various bodies in the run-up to the adoption of the resolution and the fact that fundamental problems have still not been resolved, the question also arises as to how robust the new resolution is and whether or when it will again be declared invalid by case law. There is probably no question that the ECJ will have to deal in the near future with the question of whether the EU-US Data Privacy Framework can guarantee a sufficiently high level of data protection. In this respect, it is also quite conceivable that it will again invoke the lack of adequacy of the level of data protection and declare the agreement to be ineffective with reference to its decisions on the "Safe Harbor" agreement and the "EU-US Privacy Shield". Taking this problem into account, a dual approach in the form of the additional agreement of standard contractual clauses (which in many cases already exist anyway) offers itself as a safeguard in the event that the new adequacy decision is not upheld.

As a first step, companies should check whether they work directly or indirectly with providers from the U.S. and service providers who transfer data to the U.S. If this is the case, one should then check the list provided by the U.S. Department of Commerce to determine whether the company in question is certified under the EU-US Data Privacy Framework. If it is, the data transfer can, in principle, be based exclusively on the adequacy decision. However, consideration should be given to the extent to which it would be appropriate to adopt a dual approach and base the data transfer on further safeguards in parallel. In many cases, the application of the standard contractual clauses and additional measures will already have been agreed in the past anyway and could be retained. Data protection-friendly configuration options should still be selected in any case and a risk assessment should be carried out for the specific case. If the U.S. company in question has not yet joined the agreement, it is still advisable to include the new standard contractual clauses, to take additional safeguarding measures if necessary, and to protect oneself under liability law at least in the internal relationship within the framework of the agreement on order processing, using a European service provider as an intermediary if need be. It is also advisable to document the measures taken to safeguard the data transfer in order to be able to demonstrate that the problem has been addressed.

Conclusion

In many cases, the use of American service providers has become indispensable in today's business world. However, personal data may only be transferred to a third country if it can be ensured in advance that a level of data protection comparable to that in the EU is guaranteed in the third country concerned. The EU-US Data Privacy Framework is one such way of safeguarding data transfers and simplifies data transfers to the U.S., at least for the time being. If a data transfer is to be based on the new adequacy decision, it is important to keep in mind that this does not eliminate the actual problem points and to observe how the ECJ in particular, but also the data protection authorities, position themselves in the context of the regular reviews of the agreement. In certain cases, a dual approach may be appropriate in this respect. We will be happy to support you in reviewing the processes and designing them to comply with data protection requirements.

Christina Prowald

Contact:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Christina Prowald
Research Associate

T +49 521 96535 - 980
F +49 521 96535 - 113
M christina.prowald@brandi.net