DATA TRANSFERS TO THIRD COUNTRIES

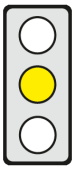
cep**PolicyBrief** No. 2017-25

Centrum für Europäische Politik

KEY ISSUES

Objective of the Communication: The transmission of personal data to third countries is to be made easier, whilst maintaining a high level of data protection, so as to promote mutual trade and effectively combat international crime.

Affected parties: EU citizens and companies that transfer or receive data from the EU, authorities.



Pro: (1) The plan to make the transmission of data to third countries easier, reduces the costs which companies incur when they want to transfer data from the EU.

(2) Only genuine convergence of the data protection level in third countries with that of the EU will ensure a truly high level of data protection. It is therefore appropriate that the Commission wants to campaign for a high level of data protection in third countries.

Contra: (1) The idea behind the adequacy decision that third countries are able to provide an "adequate" level of data protection, is currently unrealistic.

(2) Standard data protection clauses and Binding Corporate Rules only bind the participating companies. They cannot therefore prevent either access to data by secret service agencies in third countries or compensate for the lack of effective legal remedies.

CONTENT

Title

Communication COM(2017) 7 of 10 January 2017: **Exchanging and Protecting Personal Data in a Globalised World**

Brief Summary

- **Context and objectives**
  - As from May 2018, the General Data Protection Regulation [DSGVO, (EU) 2016/679; see cep**PolicyBrief**] and the "Police Directive" [(EU) 2016/680] – the latter in relation to the area of criminal prosecution – will stipulate how business and authorities may process personal data in the EU (see cep**Study** on EU data protection law). They also stipulate the requirements under which this data can be transferred to third countries and provide for familiar and new transfer tools (p. 3-6).
  - Global trade and the growing need for protection of privacy are leading to a worldwide increase in data protection legislation. At the same time, data transfer to third countries is becoming ever more important for EU companies and authorities as part of digital transformation (p. 2 and 7).
  - Varying levels of data protection and differing data protection systems in the EU and third countries, however, represent an obstacle to international data transmission (p. 2 and 11).
  - The Commission wants to promote the EU's "high standards of data protection" worldwide and lobby to bring data protection systems in third countries into line with these standards. The aim is to allow or facilitate data transfer to third countries whilst maintaining a high level of data protection so as to (p. 2-4)
    - promote free trade and
    - combat cross-border crime, and other violations, more effectively.
  - For this purpose, the Commission wants to
    - make greater use of the "transfer toolkit" of the GDPR – forming the legal basis for data transfer to third countries – (p. 6–13); these tools include
      - the "adequacy decision" with which the Commission declares the data protection level of a third country to be "adequate",
      - "alternative transfer tools" which permit data transfer without an adequacy decision.
    - promote high data protection standards at international level (p. 2–3 and 11–13) and improve the cooperation between the data protection authorities in the EU and the competent authorities in third countries (p. 12 and 13) and
    - facilitate the exchange of personal data between law enforcement authorities in order to improve cooperation on law enforcement in the EU and with third countries (p. 13–15).

- **"Adequacy decisions"**
  - Adequacy decisions are decisions with which the Commission determines, following a comprehensive assessment of the data protection system of a third country, that its data protection level is "essentially equivalent to that of the EU" and thus "adequate" (Art. 45 (1) and (3) GDPR, p. 4 and 6).
  - They facilitate the free transfer of data to a third country without the need for the data exporter to provide further safeguards or obtain any authorization (p. 4, 6).

Authors: Dr. Anja Hoffmann, LL.M. Eur. and Bastian Sattelberger | hoffmann@cep.eu
cep | Kaiser-Joseph-Strasse 266 | 79098 Freiburg | Germany | Telephone +49 (0)761 38693-107 | www.cep.eu

– They may be limited to specific geographical areas or economic sectors in a third country (p. 4)
– The Commission wants to pursue a dialogue with selected third countries on the "adequacy" of their data protection level. It wants to make the selection according to criteria such as the extent of commercial relations and data flows from the EU with the country (p. 7 and 10).
– These countries include (p. 7 and 10)
  - key Asian trading partners such as Japan, Korea and possibly India,
  - Latin American countries, in particular Mercosur countries such as Brazil and Paraguay, and
  - countries neighbouring the EU who express an interest.
– The Commission wants to pass adequacy decisions for the selected countries - country-wide or limited to certain areas or sectors (p. 7 and 10).
– It wants to assist these countries in introducing "strong" data protection provisions and endeavour to achieve convergence between their provisions and the EU standard (p. 10).
– The Commission wants to monitor and regularly review existing adequacy decisions – especially the so-called EU-US Privacy Shield framework with the USA (see cep**Study** on the Privacy Shield) – in order to take account of any changes in the level of protection in the third country (p. 8–9).

► **"Alternative tools" for data transfer**
– In the absence of an adequacy decision for a third country, data exporters can compensate for inadequate data security by way of "appropriate safeguards" by using the "alternative tools" specified in the GDPR in order to transfer data lawfully to the third country (p. 4). Alternative transfer tools include:
  - "standard data protection clauses": These are clauses in contracts between companies operating in the EU and partners in third countries. They are adopted or approved by the Commission (Art. 46 (2) (c) and (d) GDPR).
  - "binding corporate rules" (BCR): These are in-house company data protection rules for data transfers to third countries which have to be approved by regulatory authorities. They permit transfers within multinational group companies and also, as from the entry into force of the GDPR, within "a group of companies involved in a joint economic activity" (Art. 47 (1) GDPR, p. 5)
  - "approved codes of conduct" and"certification mechanisms": Companies in third countries can apply codes of conduct on data protection – that are approved by a competent European regulatory authority – or have their data protection standard certified. They give an undertaking to the data exporter in the EU by way of legal – e.g. contractual – assurances to comply with the corresponding requirements (Art. 40–42 GDPR, p. 5).
– The Commission wants inter alia to work together with industry, authorities and international organisations in order to adapt the alternative transfer tools to the needs of the individual industries, business models and economic operators and thus promote their use (p. 4-5 and 10–12).
– To promote standard data protection clauses, it proposes, in particular (p. 10- 12)
  - to adopt new clauses primarily for contracts between processors – i.e. persons, authorities or bodies that process personal data on behalf of a controller subject to data protection obligations, – or
  - to supplement existing clauses with technical or business-model-related safeguards which
    - are tailored to the requirements of a specific sector, e.g. specific safeguards for the transfer of sensitive health-related data, or
    - relate to specific processing procedures that are often used in certain third countries, e.g. outsourcing services that are carried out for EU companies.
– With regard to other alternative tools, the Commission calls for (p. 10),
  - the development of "sectoral" BCR to be developed for corporate groups involved in a joint economic activity, e.g. the travel sector, and for data transfers between processors;
  - the establishment of requirements and technical EU standards for certification mechanisms;
  - the promotion of convergence between BCR and similar corporate guidelines ("Cross Border Privacy Rules") developed by the Asia Pacific Economic Cooperation (APEC) in order to make it easier for companies to change between the two systems.

► **International cooperation on data protection**
– The Commission wants to promote high standards of data protection at global level by (p. 11 ,13)
  - using "multilateral fora" such as the G20 Summit 2017 or the United Nations to foster "a global culture of respect for data protection rights",
  - promoting "swift adoption of the modernised text" of the European Data Protection Convention [ETS No. 108] and the EU's accession thereto and by encouraging the accession of third countries.
    This Convention is a treaty under international law to which 50 countries have acceded so far. Similar to the EU data protection principles, it establishes binding rules on data protection and international data transfer and endeavours to achieve a uniformly high level of protection in the signatory states.
– The Commission wants to improve cooperation with authorities in third countries in order to facilitate the effective enforcement of data protection legislation. It is considering in particular (p. 12 - 13)
  - concluding framework agreements with important third countries – inter alia on mutual assistance ,
  - developing "international cooperation mechanisms" on the basis of Art. 50 GDPR.

- **International cooperation on law enforcement**
  - The Commission also wants to improve cooperation with third countries in the field of criminal prosecutions and other areas of law enforcement in order to facilitate data sharing with a high level of protection.
  - In particular, the Commission announces an examination of the possibilities (p. 13–16),
    - to adopt adequacy decisions for "qualified" third countries under Art. 36 (3) of the Police Directive [(EU) 2016/680] and
    - for negotiating framework data protection agreements with third countries along the lines of the agreement between the EU and the USA ("Umbrella Agreement") in order to improve data sharing in relation to criminal prosecutions and public enforcement in the area of competition/consumer protection.
  - In addition, the Commission wants to (p. 14-16)
    - facilitate the exchange of "electronic evidence", subject to data protection standards - e.g. the electronic trail left by an offender such as his IP address – and thus improve criminal justice in cyberspace;
    - examine the data protection rules of existing cooperation agreements between Europol and "third parties";
    - in relation to the exchange of Passenger Name Records (PNR, see cep**PolicyBrief**) with third countries, apply "consistent standards and specific fundamental rights protections" and work out a model agreement where appropriate.

Policy Context

In its Work Program 2017 [COM(2016) 710], the Commission already announced its intention to explore new adequacy decisions to ensure "high standards when personal data is transferred to third countries" (p. 12).

Options for Influencing the Political Process

Directorates General: DG Justice and Consumers (leading)

ASSESSMENT

Economic Impact Assessment

The Commission's **plan to make** the **transfer of data to third countries easier, tends to reduce** expenditure and thus **the costs that** European and non-European **companies** often **incur when they want to transfer data** from **the EU** to third countries in a lawful manner. These costs arise from the need to conclude contracts containing standard data protection clauses or from the costly in-house implementation of BCR for data transfers to third countries (cf. cep**Study** on the Privacy Shield) in the absence of a corresponding adequacy decision.

The tools under the GDPR – with which the Commission principally wants to achieve its aim – are basically appropriate. Their application requires caution however:

The increased use of adequacy decisions allows companies to transfer data to third countries more often without any additional authorisation. As a result, there is less of a burden on the companies concerned and they enjoy legal certainty. Adequacy decisions can, however, cease to be justified where previously unknown, major data-protection deficits in a third country become apparent or arise for the first time. In the worst case, this can result in them being declared unlawful and therefore invalid by the European Court of Justice (CJEU). This happened in the case of the former adequacy decision for the USA ("Safe Harbour"), after it was found that the American secret services had gained extensive access to the data of European citizens [cf. Schrems Judgement (C-362/14), cep**Study** on the Privacy Shield]. Affected companies are faced, in such a case, with a significant level of legal uncertainty and have to switch, sometimes at short notice, to an alternative legal basis. The monitoring and regular assessment of existing adequacy decisions, envisaged by the Commission, is therefore essential. That is the only way to recognise and counteract a fall in the data protection level in third countries at an early stage and thereby enforce a high level of data protection.

The fact that, in selecting the third countries for which it wants to conclude adequacy decisions, the Commission intends to focus on economic or political considerations – such as the extent of trade relations with a third country – tends to increase the benefit of the decisions. Such considerations and the accompanying pressure must not be allowed to undermine the data protection level however.

Adapting the alternative tools for data transfer to suit individual industries, business models and economic operators extends their area of application and facilitates their implementation and use for companies, but alternative tools alone cannot generally guarantee sufficient data protection in third countries because they only bind the participating companies and not the countries (see also Legal Assessment). Their use is therefore risky for companies because they may be liable in the EU for data protection breaches committed in a third country. In the absence of alternatives, the Commission should therefore promote the tools but work towards closing the gaps in protection by additional requirements – such as an obligation to ensure data encryption.

Ultimately – leaving aside all the tools – **only genuine convergence of the data protection level in third countries with that of the EU** will ensure **a truly high level of data protection** thus ensuring reliability with easier transference of data. **It is therefore appropriate that the Commission wants to campaign** in fora –

such as the G-20 Summit – **for a high level of data protection in third countries** and promote the EU Data Protection Convention**.**

Legal Assessment

Legislative Competency

Unproblematic.

Subsidiarity

Adequacy decisions and decisions with which the Commission adopts or approves standard data protection clauses, are implementing acts which must remain within the limits of the EU Treaties and must be adopted in the committee procedure (Art. 45 (3), 46 (2) and 93 GDPR). Insofar as the EU is exclusively competent to conclude international framework agreements, the principle of subsidiarity is not applicable.

Compatibility with EU Law in other Respects

The GDPR allows for more flexible solutions when transferring data in business or between authorities than the existing Data Protection Directive 95/46/EC. It is, however, questionable whether the strict requirements which it imposes are capable of being met in practice.

In practice, **the idea behind the adequacy decision that third countries are able to provide an** "**adequate**" **level of protection** to the required extent **is** – even more after the requirements have been precised by the European Court of Justice (CJEU) – **currently unrealistic.** This is however precisely what is required for an adequacy decision. The "Privacy Shield" decision for the USA shows which efforts and even "distortions" are necessary. In addition, due to the upcoming increase in the level of protection in the EU provided by the GDPR, in principle, all existing adequacy decisions will have to be assessed. The Commission should also give these assessments clear priority.

Alternative transfer tools such as standard data protection clauses and BCR not only have to provide "appropriate safeguards", in addition, the data subjects must have "enforceable rights and effective legal remedies" in the third country (Art. 46 (1) GDPR). In this regard, in the Schrems Judgement (C-362/14), the CJEU stipulated that the data subjects not only have to be able to defend themselves against any interference with their fundamental rights resulting from state measures, but must also be able to enforce their rights to access personal data as well as to correct it and delete it.

The CJEU has also established additional requirements for adequacy decisions which can be applied analogously to alternative transfer tools such as standard data protection clauses and BCR (cf. cep**Study** on the Privacy Shield). Inter alia, there must be effective detection and supervision mechanisms to monitor and control compliance with data protection rules. Interference with the fundamental right to protection of personal data – such as access by public authorities – must be limited to what is "strictly necessary". The latter in particular is, in practice, not only politically difficult to implement but cannot be regulated by contractual **standard data protection clauses or BCR** either, since these **only bind the participating companies** and not the third country itself or its authorities. **They cannot therefore prevent** groundless and unrestricted **access to data by intelligence agencies in third countries or compensate for the lack of effective** judicial **remedies.**

An evaluation by the EU data protection authorities addressing the question of how far standard data protection clauses and BCR are still permitted to be used at all in light of the CJEU case law, is still pending. Until there is a decision from the CJEU, the future of these tools remains uncertain. The CJEU may soon have the opportunity in proceedings pending in the Irish High Court (File No. 2016/4809P) to give an opinion on the lawfulness of the use of the standard data protection clauses for data transfers to the USA. It is not unrealistic to expect that it will also express concerns about the use of these clauses.

Data protection deficits in third countries can however be reduced if the EU also includes the necessary data protection guarantees in international agreements with third countries – e.g. a restriction of the access to personal data by national authorities or effective supervision and remedies, instead of relying in this regard – as with the "Privacy Shield" – on vague promises by foreign governments. Problematic is the fact that international agreements have effects under international law beyond that of EU law and thus – unlike adequacy decisions – cannot be declared invalid by the CJEU.

Impact on German Law

Dependent on the actual design.

Conclusion

The plan to make the transmission of data to third countries easier, reduces the costs which companies incur when they want to transfer data from the EU. The idea behind the adequacy decision that third countries are able to provide an "adequate" level of data protection, is currently unrealistic. Standard data protection clauses and BCR only bind the participating companies. They cannot therefore prevent either access to data by secret service organisations in third countries or compensate for the lack of effective legal remedies. Ultimately, only genuine convergence of the data protection level in third countries with that of the EU will ensure a truly high level of data protection. It is therefore appropriate that the Commission is advocating a high level of data protection.

Authors: Dr. Anja Hoffmann, LL.M. Eur. and Bastian Sattelberger | Telephone +49 (0)761 38693-107 | hoffmann@cep.eu