Processing of Personal Data in Third Countries

Version 1.2 | Based on the EU General Data Protection Regulation

www.bitkom.org

bitkom

Publisher

Bitkom e. V.
Federal Association for Information Technology, Telecommunications and New Media
Albrechtstraße 10 | 10117 Berlin

Contact

Susanne Dehmel | Managing Director for Law & Security
T 0049 30 27576-223 | s.dehmel@bitkom.org

Responsible Bitkom Working Group

WG Data Protection

Graphics & Layout

Kea Schwandt | Bitkom e. V.

Cover

© 12521104 – istock.com

Processing of Personal Data in Third Countries

Version 1.2 | Based on the EU General Data Protection Regulation

Table of Contents

Preface

'Transmission of Personal Data - Domestic, EU Countries, Third Countries' was the fourth publication of the Bitkom work group data protection and dates back to 2005.

The Data Protection Working Group consists of experts of Bitkom Members and deals with current topics and data protection-specific aspects of the information and communication technology. A profile of the Working Group can be found at the end of this guide.

The updated version 1.1 was developed in summer 2016 on the basis of the still applicable law of the EU Data Protection Directive 95/46 and the Federal Data Protection Act as well as taking into account the current case law on Safe Harbour. It served as an orientation for the transitional stage until the final application of the EU General Data Protection Regulation. German version available on Bitkom's website: ↗https://www.bitkom.org/Bitkom/Publikationen/Uebermittlung-personenbezogener-Daten-Inland-EU-Laender-Drittlaender-2.html

The current version 1.2 was developed in summer 2017 on the basis of the EU General Data Protection Regulation which will be applied from 25 May 2018 onwards.

For the last update, we especially thank the following members of the Working Group:

- Arnd Böken, Graf von Westphalen Attorneys at Law
- Jonas from Dall'Armi, Vodafone Kabel Deutschland GmbH
- Frank Ingenrieth, German Association Self-Regulation Information Economy (SRIW)
- Manfred Monreal, Deutsche Post AG
- Barbara Schmitz, Osram GmbH

To the original version of the guideline significant contributions were made by: Anne Bernzen, Dr. Sibylle Gierschmann, LL. M., Ulrike Schroth, Regina Wacker-Dengler, Wolfgang Braun, Helmut Glaser, Alexander Heimel, Stefan Lerbs, Ralf Maruhn, Mirko Schmidt, Florian Thoma.

Berlin, October 2017

The following further publications of the Bitkom Working Group Data Protection are available in English:

- ↗FAQ –What to know about the GDPR? September 2016.
- ↗Template Agreement Processing in behalf of a controller. April 2017.
- ↗Risk Assessment and Data Protection Impact Assessment. April 2017.
- ↗The Processing Records (Version 4.0). May 2017.
- Overview: ↗https://www.bitkom.org/Bitkom/Publikationen/FAQ-What-to-know-about-the-General-Data-Protection-Regulation-GDPR-2.html

Executive Summary

General

- **The framework conditions for data processing in third countries remain more or less the same:** The GDPR maintains the same legal possibilities for internationally operating companies for data transfers to third countries as the Data Protection Directive did (among others, consent, contract, standard data protection clauses (previously: standard contractual clauses), binding corporate rules (short: BCR) and partially new and previously approved Codes of Conducts (short: CoC) as well as approved certification mechanisms.

  Note: Companies should first consider whether an adequacy decision is in place for the country to which the data is to be transferred (see Article 45 of the GDPR). If that is the case, the data can be processed as inside the European Union. If no adequacy decision exists, companies should determine whether the data processing is subject to a statutory exemption (Article 49 of the GDPR). If that is not the case either, a sufficient guarantee must be found or provided (Article 46 of the GDPR).

- **Tighter explicit involvement of the processor:** The general principles for data transfers are expressly also applicable to processors (Article 44 of the GDPR). In general, the processor will get more responsibility in his field of accountability. The processor has his own documentation obligations (e.g. whether and to which third countries he transfers personal data and which appropriate guarantees (standard data protection clauses, BCRs, etc.) are used (Article 30(2)(c) of the GDPR) and he may also be directly liable for data breaches (Article 82 of the GDPR.

Data transfer based on an adequacy decision

- **The criteria for an adequacy decision have been extended:** The GDPR provides the criteria for adequacy decisions, which have to be taken into account by the EU Commission (Article 45(2) GDPR), such as the rule of law, respect for human rights and fundamental freedoms, effective judicial redress, and the existence and effective functioning of one or more independent supervisory authorities. Additionally, following the Schrems-Decision, adequate protection depends also on the national rules and practices of the security and law enforcement authorities concerning the access to personal data for reasons of public security.

  Note: In the EU Communication ↗EU-Communication (2017) 7 the EU Commission has announced that they will – following the agreement of the EU-US Privacy Shield – now address other regulations on data transfers into other countries outside the EU. They will evaluate whether countries such as Japan or South Korea have similarly high data protection standards as the EU. These countries have recently passed new data protection legislation and strengthened the protection of privacy.

Data transfer on the basis of a statutory exemption clause

- **Exception: overriding legitimate interest:** The GDPR contains a new legal basis for a non-repetitive data transfer based on compelling legitimate interests of the controller, but only for exceptional circumstances and under specific requirements, e.g. among others, the controller shall inform the supervisory authority (Article 49(1), (2) and (6) of the GDPR).

  Example: This exception can be used, for example, when authorities in a third country (e.g. the US Department of Justice) request personal data of companies based in the EU.

  Example: Remote maintenance/trouble support in exceptional circumstances (e.g. cyber attacks) by a services provider in a third country, if access to personal data is not impossible and the controller did not conclude standard contractual clauses or cannot conclude them quickly enough.

Data transfer based on a sufficient guarantee

- **Explicit recognition of BCR as sufficient guarantees:** The GDPR expressly recognizes BCR as sufficient guarantees for data transfers to countries without adequate protection levels (Article 46 (2) (b) of the GDPR). Until now, BCR were not explicitly listed in the Data Protection Directive. The requirements of BCR have been defined by the Article 29 Data Protection Working Party (hereinafter WP29). They have now been transferred into the GDPR to a large extent.

- **Extended application of BCR to groups of enterprises engaged in a joint economic activity:** The circle of potential users of BCR has been significantly expanded. Whereas BCR were previously focused on a group of undertakings (Group), BCR are now also open to groups of enterprises that share a joint economic activity (Article 20(4) of the GDPR).

  Example: For example, different participants in the travel industry can conclude a common BCR.

- **Sufficient guarantees were extended:** The possibilities regarding sufficient guarantees were extended and do now include not only standard contractual clauses and BCR but also approved Codes of Conduct and certifications (e.g. data protection seals and marks) (Article 46(2) (e) and (f) of the GDPR).

  Example: Controllers outside of the EU can, for example, follow an EU Code of Conduct or undergo certification, which lead to the binding and enforceable obligation to comply with the data protection regulations that these instruments stipulate (see Article 42(2) of the GDPR). This is intended to support the development of customized solutions for international data transfers, e.g. for specific characteristics and need of a particular sector or industry or certain data streams.

- **Standard contractual clauses as sufficient guarantees can now also be proposed by data protection supervisory authorities:** Standard contractual clauses can now also be proposed by an EU supervisory authority. The proposed clauses shall be agreed upon with other supervisory authorities in a coherence procedure and require the approval of the EU Commission, which will apply an EU audit procedure for this purpose following Article 93(1) of the GDPR.

  Note: According to EU Communication COM (2017) 7, the EU Commission is working with the WP29, which will be replaced by the European Data Protection Board from 2018 onwards, to develop standard contractual clauses for the use between processors ('processor-to-processor standard contractual clauses'). There are currently no standard contractual clauses in place for the use between processors, but only two different types of clauses between controllers ('controller-to-controller standard contractual clauses') and a set for the use between controller and processor ('controller-to-processor standard contractual clauses').

Overview of the GDPR's System for Data Transfers

<table>
<tr><td colspan="7">Transfer to third countries according to the GDPR (Art. 44 - 49)</td></tr>
<tr><td rowspan="8">Third countries with adequacy decision Art. 45</td><td colspan="6">Third countries without adequacy decision</td></tr>
<tr><td colspan="5">Data Transfer based on sufficient guarantees, Art. 46</td><td>Conditions according to Art. 49</td></tr>
<tr><td rowspan="6">BCR, Art. 46 para 2(b), Art. 47</td><td rowspan="6">Standard contractual clauses COM Art. 46 para 2(c)</td><td rowspan="6">Standard contractual clauses supervisory authority Art. 46 para 2(d)</td><td rowspan="6">Approved codes of conduct, Art. 46 para 2(e), Art. 40</td><td rowspan="6">Certifications, Art. 46 para 2(f), Art. 42</td><td>Consent Art. 49 para 1(a)</td></tr>
<tr><td>Performance of a contract or pre-contractual measures or contract is concluded in the interest of the data subject Art. 49 para 1(b) and (c)</td></tr>
<tr><td>Transfer is necessary for important reasons of public interest Art. 49 para 1(d)</td></tr>
<tr><td>Transfer is necessary for the establishment, exercise or defense of legal claims Art. 49 para 1(e)</td></tr>
<tr><td>Protection of vital interests Art. 49 para 1(f)</td></tr>
<tr><td>Transfer is made from a register Art. 49 para 1(g)</td></tr>
<tr><td colspan="6">Transfer is necessary for the purposes of compelling legitimate interests pursued by the controller</td></tr>
</table>

1 Introduction: The Transfer of Personal Data

1 Introduction: the Transfer of Personal Data

The transfer of personal data accompanies the initiation and processing of business transactions on a daily basis. Just like the business itself, data transmission has long since ceased to stop at the borders of Germany, but is often carried out across borders between European countries or internationally. Through the increasing mobility and the globalization of world trade, this cross-border data exchange is gaining importance. This trend is further advanced by the rapid development of information technology: the worldwide communication via interconnected networks, which can be used to provide a fast and cost-effective solution for the large data volumes exchanged, has freed data processing from geographic limitations. This does not only apply to the exchange of data between contractual partners, but also the exchange and transmission within a corporate group. In international corporations, for example, personnel data is often transferred between subsidiaries and the group holding company or between the subsidiaries. Through the networks in production and trade relations, personal data is not only kept within the company or group of companies, but is also transferred to foreign companies or international databases. It is, for example, required for travel bookings to transfer employee data to a large number of third parties. Often, transfers are also necessary with regard to outsourcing projects, namely to computing service providers.

However, not all parties involved are always familiar with the legal requirements of data transfers. Nevertheless, the requirements should be taken seriously by every company. A data transfer that does not meet the legal requirements can be fined as an administrative offence with fines of up to EUR 20 000 000 or, in the case of a company, of up to 4 % of its total annual global turnover of the previous year, whichever amount is higher (Article 83(5) of the GDPR).

Against this background, the Bitkom publication ‘Processing of Personal Data in Third Countries’ aims at giving practical assistance for the day-to-day use when transferring data. In addition to a brief description of the legal framework for data transmissions (Chapter 2), data processing in third countries with an adequate level of data protection (Chapter 3), and without an adequate level of data protection (Chapter 4) will be explained. The different constellations are illustrated with a short case study. It also addresses data transmissions in a Group (Chapter 5). Finally, the guide provides supplementary materials (Chapter 6), links and references (Chapter 7).

Please note: In light of the complexity of the subject matter, the guide cannot claim completeness. In addition, the material depicted is the subject of the ongoing development of the law and subject to technology. Ultimately, this guide is therefore intended as an introduction and presents exemplary possibilities for action. Therefore, the involvement of professional in-house or external consultants is not precluded.

2 Legal Framework

2 Legal Framework

2.1 Scope of the General Data Protection Regulation

The General Data Protection Regulation (GDPR)(EU) 2016/679 of the European Parliament and of the Council and the Data Protection Directive (EU) 2016/680 were adopted on 27 April 2016, the GDPR will come into effect on the 25 May 2018, the Data Protection Directive 2016/680 has to be implemented in the Member States by the 06 May 2018. The GDPR establishes a uniform data protection law within the European Union. As a Regulation, it has direct effect and does not have to be implemented into national laws. This means that data processing in other EU countries is to be treated the same way as within Germany. The same applies to the EEA countries Norway, Iceland, Liechtenstein, as the GDPR is directly applicable there as well by means of the EEA-Agreement. These countries are therefore considered as countries within the EU with regard to data transfers.

The text of the GDPR is available ↗here in all official EU languages.

In principle, the GDPR applies to all public authorities of the EU member states and to all companies in the private sector which have a branch within the European Union. Under certain conditions, it does also apply to undertakings not established in the European Union (see section 2.4). The Data Protection Directive 2016/680 applies to the police and judicial sector and requires national implementation.

Furthermore, the application of the GDPR is subject to the condition that all or part of the personal data is processed in an automated way. For the non-automated processing of personal data, the GDPR applies if the data is stored or shall be stored in a file system (Article 2(1) of the GDPR).

2.2 Remaining Room for Regulation

The GDPR aims to harmonize data protection law within the EU. The Member States have little room left for their own regulation. There are some areas, however, where Member States are required to introduce legislation on e.g. the question of which authority the Member State appoints for representation in the European Data Protection Board. In other areas, such as employee data protection, the Member States can, within certain limits, impose additional or more detailed rules. The German legislator passed the Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 (DSAnpUG-EU) in order to make use of the remaining leeway and at the same time carrying out the necessary implementation of the Data Protection Directive. The Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 will enter into force at the same time as the GDPR in May 2018.

The text of the DSAnpUG-EU is available ↗here (German and English versions):

To a very limited extent, the GDPR allows for the EU Commission to be able to specify certain regulations in the form of so called delegated acts, Article 92 of the GDPR.

As a Regulation, the GDPR takes precedence over national law. German laws that are not adapted until then, will no longer be applicable as of May 2018.

2.3 Specific Data Protection Laws

In the public sector, the most important areas regulated by specific laws are the protection of public security, law enforcement and intelligence services. The GDPR does not apply to these subject matters. The prosecution sector, the enforcement sector, and the protection of public security are governed by the Directive (EU) 2016/680, which has been implemented in particular by the DSAnpUG-EU (Part 3, p. 45 ff.).

The EU has no legislative competence in the field of intelligence services. In this area, the Member States alone have the regulatory competence. Hence, the DSAnpUG-EU is making changes in this field regarding various specific data protection laws, e.g. the Military Counterintelligence Act (Gesetz über den Militärischen Abschirmdienst), the Federal Intelligence Service Act (Gesetz über den Bundesnachrichtendienst), the Security Screening Act (Sicherheitsüberprüfungsgesetz), and the so-called Article 10 Act (Artikel-10-Gesetz).

For the economy, the most important areas regulated by specific data protection laws are data processing in the internet, which is regulated by the Telemedia Act (Telemediengesetz, TMG), and data processing in telecommunications, which is governed by the Telecommunications Act (Telekommunikationsgesetz, TKG). Currently, the EU legislator is working on a Regulation, the Regulation of the European Parliament and of the Council on respect for private life and the protection of personal data in the electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM (2017) 10, which will harmonize such processing throughout the EU. At the time of this publication, negotiations at EU level are not yet closed.

Another important field of specific data protection laws is employee data protection, which will continue to be regulated by Member States Laws.

2.4 Territorial Scope of the GDPR

The GDPR is based on two principles: the ‘establishment principle’ and the ‘market location principle’ (Article 3 of the GDPR).

The Regulation applies to data processing in connection with the activities of an establishment of a controller or processor in the EU, regardless of whether the processing takes place in the EU or not. A branch is any permanent establishment from which a business activity is carried out, for example from a rented office, even if the activity is only marginal (cf. CJEU, judgment of 1/10/2015, Weltimmo, C-230/14).

Example: Company Inc. (C) is headquartered in New York and has an office in Berlin. The customer database of the German branch is stored on servers of the company in the USA. The GDPR applies according to Article 3(1) of the GDPR.

In accordance with the market location principle (Article 3(2) of the GDPR), the GDPR also applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

- the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
- the monitoring of their behavior as far as their behavior takes place within the Union.

Example: Company (A) based in China and without a branch office in Europe offers goods which are also delivered to buyers in Germany. For data processing, Article 3(2) of the GDPR applies.

The provision applies irrespective of whether a payment of the data subject is required.

For the applicability of the GDPR, it is sufficient that the behavior of users based in Europe is monitored. As the use of cookies on websites is already considered as behavioral monitoring, the application scope is very broad. It is also sufficient if the website service is also aimed at a user from the EU.

2.5 System of Data Protection Law

For the processing of personal data, the general principle is the so-called prohibition principle. Hence, a statutory rule-exception-relationship applies, meaning that, in general, the processing is prohibited unless it is exceptionally permitted.

Principles for the processing of personal data

The GDPR lays down the following principles for the processing of personal data (Article 5(1) of the GDPR):

a. Lawfulness, fairness and transparency
b. Purpose limitation
c. Data minimization
d. Accuracy

e. Storage limitation
f. Integrity and confidentiality

The controller must demonstrate compliance with these principles ('Accountability', Article 5(2) of the GDPR).

2.5.1 Legal Bases

The processing of personal data is only lawful if at least one of the following requirements of Article 6(1) of the GDPR is met:

a. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
b. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
c. processing is necessary for compliance with a legal obligation to which the controller is subject;
d. processing is necessary in order to protect the vital interests of the data subject or of another natural person;
e. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
f. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

For the private sector, especially consent, contract performance, fulfilment of a legal obligation, and protection of legitimate interests are of particular importance.

2.5.2 Consent according to Article 7 of the GDPR

According to the GDPR, consent must be given by means of a clear affirmative action. In contrast to the German Federal Data Protection Act, the GDPR no longer requires the written form.

However, since the controller must provide proof of consent, it is reasonable to require written consent from the data subjects, which can also be provided electronically (according to s. 36(2) subpara (3) of the Federal Data Protection Act consent of employees must be provided in written form; for more information see 5.3.1.).

If the data subject's consent is given in the context of a written declaration which also concerns other matters, such as general terms and conditions, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language (Article 7(2) of the GDPR). This requires, for

example, bold type printing or a separate text passage with its own box, which the person concerned must check separately.

The consent must be given voluntarily. This does also take into account whether the provider of a contract makes the conclusion of the contract dependent on consenting to a data processing that is not necessary for the fulfilment of the contract.

Overall, the requirements for consent are very high. Companies should review their previous models for consent and check whether they meet the new requirements. Where appropriate and necessary, they should adapt these models to comply with the new requirements by May 2018.

3 Data Processing in a Third Country with an Adequate Level of Data Protection

3 Data Processing in a Third Country with an Adequate Level of Data Protection

In principle, the GDPR assumes that the transfer of data to foreign countries outside of the EU/EEA can only be carried out if an adequate level of data protection is ensured.
This level of protection is ensured, inter alia, if

- the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection, Article 45(1) of the GDPR.

If the data protection level of a country is not secured by uniform laws, an adequacy status within the meaning of Article 45 of the GDPR shall be assumed, however, if an agreement with the EU has been made, which secures a sufficient level of data protection and the recipient of transferred data has joined the agreement (for example, Privacy Shield of the EU and the USA, see 5.6.)

Information

A chart of the possibilities for transfers to third countries can be found in section 7.5!

3.1 Assessment of Adequacy

The assessment of adequacy is made by the EU Commission in a formal procedure (Article 45 of the GDPR). This has not changed in comparison to the Data Protection Directive 95/46/EC.

However, the regulations are more detailed in many respects:

- **The evaluation criteria for adequacy decisions have been extended:** The GDPR establishes the criteria for adequacy decisions to be taken into account by the EU Commission (Article 45(2) of the GDPR) such as the rule of law, respect for human rights and fundamental freedoms, effective judicial redress, and the existence and effective functioning of one or more independent supervisory authorities. Additionally, following the Schrems-Decision, adequate protection depends also on the national rules and practices of the security and law enforcement authorities concerning the access to personal data for reasons of public security.

- **Adequacy not only for a third country, but also for one or more territories or one or more specific sectors in the third country:** According to Article 45(3) of the GDPR an adequacy decision can also be related to a territory (e.g. countries with a federal structure, such as the USA)[1] or one or more specific sectors (e.g. private sector or certain economic activities). Previously, this was not provided for in the Directive 95/46/EC:

Note

The adequacy of a data protection level does not necessarily mean that the conditions are homogenous or equivalent.

1 EU-Commission, FAQ on Commission's adequacy finding on the Canadian Personal Information Protection and electronic Documents Act, question 'Does the Commission Decision also cover provincial legislation',
↗http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/third-countries-faq/index_en.htm

3.2 Adequacy Decisions

An adequate level of data protection has been confirmed by the EU Commission in a formal decision for the following countries:

- Argentina (2003/490/EC)
- Andorra (2010/625/EU)
- Guernsey (2003/821/EC)
- Isle of Man (2004/411/EC)
- Jersey (2008/393/EC)
- Kanada (2002/2/EC)
- New Zealand (2013/65/EU)
- Israel (2011/61/EU)
- Switzerland (2000/518/EC)
- Faroe Islands (2010/146/EU)
- Uruguay (2012/484/EU)

Further information on the Commission's decisions can be found at the ↗EU-Data-Protection-Website

Example: Entrepreneur D with his registered office in Germany transfers customer data to the Company A with an adequate level of data protection (e. g. Switzerland, Guernsey, Argentina, Canada, etc.).

Decisions on adequacy adopted by the Commission in accordance with Article 25(6) of Directive 95/46/EC or new adequacy decisions based on the GDPR remain in force until they are amended, replaced or repealed by a decision of the EU Commission. They are subject to continuous monitoring by the EU Commission (audit at least every 4 years), which must initiate an investigation procedure if it has information that no appropriate level of data protection is maintained.

3.3 Future Developments

In the ↗EU-Communikation (017) 7 the EU Commission announced that they will now address other regulations on data transfers into other countries outside the EU. They will evaluate whether countries such as Japan or South Korea, the most important trading partners in East- and Southeast Asia, and (depending on the progress regarding the modernization of data protection laws) India, have similarly high data protection standards as the EU.

The EU Commission launched an ↗official dialogue on data protection and cross-border data traffic with Japan in March 2017.

On July 4, the EU Commissioner Věra Jourová and the head of the Japanese supervisory authority Haruhi Kumazawa announced in a ↗joint communication, that a mutual adequacy decision shall be made until the beginning of 2018.

Other countries in Latin America (Mercosur countries) and countries in the European Union's neighborhood[2], that have expressed an interest in an adequacy decision will also be evaluated by the EU Commission.

2 The European Neighbourhood policy covers Egypt, Algeria, Armenia, Azerbaijan, Belarus, Georgia, Israel, Jordan, Lebanon, Libya, Morocco, Moldova, Palestine, Syria, Tunisia and Ukraine.

4 Data Transfers to a Third Country without an Adequate Level of Data Protection

4 Data Transfers to Third Country Without an Adequate Data Protection Level

4.1 Legal Bases for Specific Situations (Article 49 of the GDPR)

Data transfers may also be possible in cases where an adequate level of data protection has not been established for the third country. Article 49 of the GDPR formulates exceptions ('derogations') under which circumstances personal data can be transferred to a third country without an adequate level of protection. The most important cases of Article 49 of the GDPR, including transfers for contract performance and consent of the data subject, are explained in this section.

4.1.1 Necessary Transfer for the Performance of a Contract

Data transfers to a third country without an adequate level of data protection is exceptionally allowed if a contract has been concluded between the data subject and the controller, and the data transfer is necessary for the performance of this contract, Article 49(1)(b) of the GDPR. This shall also apply if the transfer is necessary for the implementation of pre-contractual measures taken at the request of the data subject.

In practice, this exception is, in addition to international payment transactions and distance selling sales contracts, primarily used in the tourism industry. This enables the implementation of contractual agreements on international transport services, reservations of rental cars, accommodation, or hotel rooms in third countries.

Example: Customer (C) wants his travel agency to reserve a hotel room for him or her in Beijing. The travel agency transfers the data of (C) to the hotel in Beijing on basis of Art. 49(1)(b) of the GDPR, as the transfer is absolutely necessary for the performance of the contract between (C) and the travel agency.

A contract within the meaning of section b could also be an employment contract so that the transfer of employee data to a third country may be permitted on the basis of an employment contract. The decisive factor for assessing the legitimacy is whether the transfer is necessary for the execution or fulfilment of the respective individual regulations of the employment contract. This must be checked separately for each employee. The legitimacy of data transfers is conceivable, for example, if the employee is obliged to work abroad or when the employee is granted stock rights that are managed in a third country.

Slightly different are cases covered by Article 49(1)(c) of the GPDR which can justify a data transfer. According to section (c) a transfer may be permitted if it is necessary for the performance of

Notice

The legal requirements for a transmission according to Art. 6 of the GDPR within the EU are also relevant for a data transfer to a third country, because in addition to the attention of special conditions of international data transfers, it must be assessed whether the transmission (data processing) meets the general conditions of the GDPR.

A TWO-STAGE EXAMINATION is therefore required.

a contract which has not been concluded between the data subject and the controller, but which is concluded in the interest of the data subject between the controller and another third party.

Example: An employer transmits data of an employee for whom he took out an insurance with a foreign insurance company. In Germany section (c) often covers contracts for the benefit of third parties within the meaning of s. 328 BGB (German Civil Code).

4.1.2 Data Transfer on the Basis of Consent

As in the case of data transfers within Germany or within the EU/EEA, data transfers to a third country may also be allowed on the basis of the consent of the data subject, Article 49(1)(a) of the GDPR. The strict requirements of consent set out in part 2.4.2 also apply in this case.

However, there is another difficulty with data transfers to third countries as according to Article 49(1) (a) of the GDPR, the data subject (in addition to the above-mentioned circumstances) must be fully informed about the possible risks of such transfers. Transparency is therefore required with regard to safeguards and data protection guarantees provided by the recipient or in the recipient country.

4.1.3 Data Transfer on Basis of Compelling Legitimate Interests

For narrowly defined exceptional situations, Article 49(1) sentence 2 of the GDPR, permits transfers to a third country without an adequate level of protection. Accordingly, the transfer may be authorised if it is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interest of the rights and freedoms of the data subject, and if the controller has assessed all circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. In addition, the controller must inform the supervisory authority and the data subject. The assessment and the suitable safeguards should be documented in the processing records pursuant to Article 30 of the GDPR.

The scope of this exception is very narrow. Recital 113 of the GDPR refers to scientific or historical research purposes or statistical purposes. If a transfer is to be based on this exception, the controller should contact the competent supervisory authority in advance.

4.1.4 Data Transfer for the Establishment, Exercise or Defence of Legal Claims

In contrast to Directive 95/46/EC, the GDPR contains an explicit provision for cases where a court or authority of a third country requires the transfer of personal data.

Article 48 of the GDPR stipulates that these judgments or administrative decisions may only be recognised and enforceable within the EU if they are based on a mutual legal assistance agreement or another international agreement between the third country and the Union or a Member State. This can be, for example the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, or international agreements on cooperation in the fight against crime and prosecution.

Where the judgment or administrative decision cannot be based on mutual assistance agreement or other international instruments, the transfer of data cannot be justified. The general principles then apply: the transfer is only legitimate if there is a legal basis for a transfer and an appropriate level of protection exists in the third country, or an exception according to Article 49 of the GDPR applies.

4.2 Appropriate Safeguards – Introduction

In the absence of an adequacy decision, appropriate safeguards for the protection of data subjects can compensate for the lack of data protection in the third country. Article 46 of the GDPR distinguishes between safeguards which do need (para. 2) and do not need approval (para. 3).

Safeguards without special approval of the supervisory authorities may be:

a. A **legally binding and enforceable instrument between public authorities or bodies**;
b. **Binding corporate rules** in accordance with Article 47 of the GDPR;
c. **Standard data protection clauses** adopted by the Commission in accordance with the examination procedure referred to in Article 93(2) of the GDPR;
d. **Standard data protection clauses** adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2) of the GDPR;
e. **Approved codes of conduct** pursuant to Article 40 of the GDPR together with binding and enforceable commitments of the controller or processor in the third country to apply appropriate safeguards, including those with regard to the data subject's rights;
f. **Approved certification mechanism** pursuant to Article 42 of the GDPR together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including those with regard to the data subjects' rights.

The safeguards listed in Article 46(3) of the GDPR are subject to approval by the competent supervisory authority. The following safeguards are part of such an approval procedure:

a. **Contractual clauses** between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation;
or
b. **Provisions to be inserted into administrative arrangements** between public authorities or bodies which include enforceable and effective data subject rights.

The purpose of the safeguards is to ensure that the data protection regulations and the rights of the data subject are adequately respected.

4.3 Standard Data Protection Clauses, Article 46(2)(c) and (d) of the GDPR

According to Article 46(2) of the GDPR, data transfers to a third country may also be based on standard data protection clauses of the Commission (lit. c) or the supervisory authority (lit. d). This possibility is also already included in Article 26(4) of Directive 95/46/EC, but the Directive only recognises the possibility of adopted clauses by the Commission. The GDPR provides that also supervisory authorities can develop standard data protection clauses, which must be approved by the Commission in an examination procedure.

Based on Article 26(4) of Directive 95/46 EC, the Commission had adopted standard contractual clauses for different case scenarios:

- Standard contractual clauses for data transfer between controllers **(controller-controller-transfer)**
  - Set I from Decision 2001/497/EC of 15 June 2001
  - Set II ('alternative standard contractual clauses') from Decision 2004/915/EC of 27 December 2004 amending Decision 2001/497/EC
- Standard contractual clauses for the transfer of data between controllers responsible for data processing and processors processing on behalf the controllers **(controller-processor-transfers):**
  - Decision 2010/87/EU of 5 February 2010 (the former standard contractual clauses on data processing on behalf from Decision 2002/16/EC of 27 December 2001 apply only to contracts concluded before 15 May 2010)

Whereas there is only one type of standard data protection clauses for data transfers between controllers and their processors, there is a choice of two sets for data transfers between controllers. These differ in particular with regard to liability, the binding nature of information or decisions by supervisory authorities and the room for leeway and additions.

Note

Article 26(4) of Directive 96/46/EC refers to **'standard contractual clauses'**, whereas the GDPR now refers to such safeguards, provided by the Commission or supervisory authority to compensate for the lack of data protection in a third country, as **'data protection clauses'** (see. e.g. Article 46(2) of the GDPR).

However, due to the limited liability and duty of disclosure of the data exporter and the resulting restrictions of German law, Set II is not suitable for the transfer of employee data.[3] Set II was negotiated by the International Chamber of Commerce (with the participation of other business associations) with the objective to address weaknesses in the standard contractual clauses of June 2001. These 'alternative clauses' are therefore considered to be preferable by many companies.

↗Set I (2001/497/EG from 15/6/2001)	↗Set II (2004/915/EG from 27/12/2004), alternative clauses
Joint and several liability *see. clause 6*	Each party is liable for its own fault; punitive damages are excluded; *see. paragraph III* But: not suitable for employment data due to limitation of liability (at least in Germany)
Stricter commitment to (non-binding) advice of supervisory authority *see. clause 5*	Commitment to binding decisions of the supervisory authorities; *see. paragraph V*
Prohibition to change clauses *see. clause 11*	Permission to conclude supplementary contracts to deal with commercial issues; Description of the transmission in Annex B, may be adapted and supplemented; *see. paragraph VII*

When using standard data protection clauses, care should be taken to ensure that the contractual partners do not change or otherwise restrict the specified clauses through a side agreement.

Amendments are only allowed within the scope of so-called business clauses, insofar as the relevant standard data protection clauses permit such an addition and as long as these do not directly or indirectly contradict the standard data protection clauses or violate fundamental rights or freedoms of the concerned data subjects.

In the event of an unauthorized modification, the clauses lose their privileged status as standard data protection clauses within the meaning of Article 46(2) of the GDPR and are then subject to approval as 'simple' contractual clauses. If the transfer is based on (unmodified) standard data protection clauses, German data protection law does not require the approval of the supervisory authority, as the EU Commission already approved that the clauses provide sufficient safeguards for the data protection rights of data subjects during its examination procedure pursuant to Article 93(2) of the GDPR (or Article 26(4) in conjunction with Article 31(2) of Directive 95/46/EC). However, regulatory authorities may require the submission of agreed standard data protection clauses.[4]

Note

In other EU states (e. g. AT, HR, CY, EE, FR, IS, LV, LT, LU, MT, RO, SI, ES) authorisation by the supervisory authority was sometimes required under the Data Protection Directive, even in the case of standard contractual clauses. This is no longer necessary after the adoption of the GDPR.

3 See Coordinated positions of the German supervisory authorities in the working group 'International Data Traffic' of 12/13 February 2007, page 2, II.2.

4 Further information on the subject of standard contractual clauses see Schmitz/v. Dall'Armi, ZD 2016, 217ff.

Excursus: Applicability of the Standard Contractual Clauses after the CJEU Ruling on Safe Harbour of 6 October 2015

With the 'Safe Harbor' decision, the EU Commission had created the basis for establishing an appropriate level of data protection within the meaning of Article 25(2) Directive 95/46/EC for the transfer of personal data to the US, if the data importer in the US complies with the Safe Harbour Principles and the so-called 'Frequently Asked Questions'. However, the CJEU has declared this agreement invalid with its decision of 6 October 2015 (the so-called 'Schrems ruling'). As a result, the transfer of data to the US on the basis of the Safe Harbour decision is no longer permitted since the end of January 2016 at the latest (see ↗the WP29).

According to the majority opinion of the supervisory authorities, the literature and the EU Commission, standard data protection clauses have not per se lost their validity with the CJEU ruling and can therefore still be used for the time being. In particular, the CJEU alone has the competence to declare a Commission decision invalid. As long as such conclusion is not drawn, the Commission's decision is binding for all institutions of the Member States in accordance with Article 288(4) of the TFEU (see CJEU, judgment of 6 October 2015, Schrems, C362/14, RZ 51).

However, the validity or compatibility of existing standard contractual clauses with European law remains the subject of legal proceedings and discussions. For example, the Irish High Court is currently dealing with a process on data transfers from Facebook to the US (also known as Schrems II), whereby the Irish Data Protection Commissioner (DPC) generally wants the CJEU to clarify the question of the legitimacy of data transfers to third countries by means of standard contractual clauses (cf. Irish High Court, Schrems II, Az. 2016/4809P). The hearings of the parties involved in the process took place from July 2016 to January 2017.

Update!

The Irish High Court, on October 3, 2017, endorses the decision of the Irish Data Protection Commissioner to seek a referral to the CJEU and supports much of the analysis deployed by the DPC. The specific details and wording of the questions to be referred have yet to be formulated. The Court addresses different areas in its judgement where references could be possible e.g. what is the correct 'comparator' law for an Article 25 of the Data Protection Directive 95/46/EC adequacy assessment, whether US law respects the essence of Article 47 of the GDPR and whether the Privacy Shield Ombudsperson mechanism is sufficient, or whether the ability of data protection authorities to suspend data transfers in Art. 4 of the Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (2010/87/EU) in combination with Art. 28 of the Data Protection Directive 95/46/EC is sufficient to secure the validity of the Standard Contractual Decisions. Once the reference to the CJEU is officially made, it will be for the CJEU to fix a hearing date. It seems likely that the case will be given priority (as with the Safe Harbour challenge in Schrems I). More information on this procedure and the judgements can be found on the website of the Irish Data Protection Authority. ↗https://www.dataprotection.ie/docs/EN/03-10-2017-Irish-High-Court-grants-the-Data-Protection-Commissioner-its-CJEU-referral-in-DPC-v-Facebook-Ireland-and-Maximilian-Schrems/m/1666.htm

4.4 Individual Contractual Clauses, Article 46(3)(a) of the GDPR

The data exporter, who can be either controller or processor, can conclude an individual, i. e. self-formulated contract on data protection with the controller, processor or recipient resident in the third country, which must be approved by the competent supervisory authority - in the case of postal and telecommunications companies by the Federal Commissioner for Data Protection and Freedom of Information (BfDI) in Germany -. This possibility of implementing appropriate safeguards was already provided for in Directive 95/46/EC in Article 26(2).

4.5 Binding Corporate Rules

4.5.1 Introduction

The European legislator has explicitly included 'binding corporate rules', in the list of 'appropriate safeguards' to ensure an adequate protection of data being processed in countries without an appropriate data protection level, Article 46(2)(b) of the GDPR. Appropriate safeguards are intended to compensate for the fact that personal data is processed in a country which has no (identified) adequate level of data protection, Recital 108. The aim is to ensure as far as possible

that personal data are also processed in accordance with the principles of the GDPR and that data subjects can enforce their statutory rights.

Note!

The purpose of 'appropriate safeguards' is - only - to compensate for the transfer of personal data to 'unsafe third countries'. Therefore, the general requirements for legally compliant data processing must always be met when processing personal data. Recital 48 sentence 2 of the GDPR makes this clear. Therefore, a processing of personal data always requires a legal basis as laid down in Article 6(1) of the GDPR. Also in the case of intra-group data processing on behalf of the controller, a contract in accordance with Article 28 of the GDPR needs to be concluded (see also 6.6.3).

To a large extent, the GDPR includes the same legal requirements as those specified by the WP29 which has published several working papers (WP) about BCR over the past twenty years. From a legalistic view, BCR are neither a contract nor a code of conduct, but rather an instrument of 'self-regulation of industry' (WP 12). BCR were characterized by the fact that they are binding and legally enforceable, intended for internal use within the group of undertakings and designed for international data transfers (WP 74). The central element was the unilateral declaration of self-obligation by the company management to observe the principles of European data protection law for processing operations outside the European Union. However, the declaration of voluntary commitment is also a certain shortcoming, because it is not regarded as a unilateral declaration of intent and is not regarded as legally binding in all legal systems (WP 74). This acceptance problem is likely to have been resolved by explicit inclusion in the GDPR, at least for the EU Member States. While standard contractual clauses cover single transfers to individual recipients, BCRs provide a lasting safeguard for countless transfers to one or more recipients. These special requirements (see 5.4.3) are derived from characteristics of BCR, which interested users must fulfil.

4.5.2 Definition

Binding corporate rules are, according to the legal definition in Article 4 No. 20 of the GDPR 'personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.'

In this way, the legislature has shifted away from the concept of 'company-internal' rules and made BCR into 'internal' rules for companies that may not have a common controlling 'corporate management'.

4.5.3 Requirements

Article 47 of the GDPR contains a long list of requirements that must be met by BCR. Many of the requirements are vaguely formulated and leave room for interpretation. In interpreting the requirements, the supervisory authorities will use their working papers published in recent years, some of which contain very precise statements on the implementation of individual requirements. WP 153 contains statements on the requirements to be fulfilled in the BCR and where further information on the requirements can be found. The following table tries to give an overview:

Requirements	To fulfil in BCR?	Comment
Art. 47(1)(a): BCR are legally binding and apply to and are enforced by every member concerned of the group of undertakings or group of enterprises, including their employees.	Yes	WP 153 point 1.1 and 1.2
Art. 47(1)(b): Expressly confer enforceable rights on data subjects with regard to the processing of their personal data	Yes	WP 153 point 1.3
Art. 47(2)(a): Structure and contact details of the group of undertakings or group of enterprises engaged in a joint economic activity and each of its members	No	WP 153 point 6.2
Art. 47(2)(b): Description of the relevant data transfers or set of data transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question	Yes	WP 153 point 4.1
Art. 47(2)(c): Internal and external legally binding nature of the BCR	Yes	WP 153 point 1.1 and 1.2
Art. 47(2)(d): The application of general data protection principles, in particular purpose limitation, data minimization, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security and requirements of onward transfers to bodies not bound by the BCR	Yes	WP 153 point 6.1
Art. 47(2)(e): The rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to a decision based solely on automated processing, including profiling in accordance with Article 22 as well as the right to lodge a complaint with the competent authority and before the competent courts of the Members State in accordance with Article 79, and to obtain redress and, where appropriate, compensation in the event of a breach of the BCR	Yes	WP 153 point 1.3
Art. 47(2)(f): The acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the BCR by any member concerned not established in the Union; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage.	Yes	WP 153 point 1.6

Requirements	To fulfil in BCR?	Comment
Art. 47(2)(g): How the information on the BCR, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 13 and 14	Yes	WP 153 point 1.7 Member States may impose special transparency requirements for the use of BCR for employee data, Art 88 (2) GDPR.
Art. 47(2)(h): The tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge for the monitoring compliance with the BCR within the group of undertakings or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaints-handling	Yes	WP 153 point 2.4
Art. 47(2)(i): The complaint procedures	Yes	WP 153 point 2.2
Art. 47(2)(j): The mechanisms within the group of undertakings or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the BCR. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subjects. Results of such verification should be communicated to the person or entity referred to in (h) and to the management board of the controlling undertaking of a group of undertakings or enterprises engaged in a joint economic activity and should be made available upon request to the competent supervisory authority	Yes	WP 153 point 2.3
Art. 47(2)(k): The mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority	Yes	WP 153 point 5.1
Art. 47(2)(l): The cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j)	Yes	WP 153 point 3.1
Art. 47(2)(m): The mechanisms for reporting to the competent supervisory authority of any legal requirements to which a member of the group of undertakings or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the BCR	Yes	WP 153 point 6.3
Art. 47(2)(n): The appropriate data protection training for personnel having permanent or regular access to personal data	Yes	WP 153 point 2.1

Consideration!

These requirements, which have been developed and established by the WP29 over many years, are based on the premise that they apply to a group of undertakings with a central and controlling body. Due to the expansion of the user group and the partial lack of acceptance of BCR in some legal systems, it can be reasonable for interested parties to consider designing their BCR as a multilateral contract.

Advice!

The Working Papers of the WP29are also valid after 25 May 2018 and contain many interesting explanations. Particularly noteworthy is the WP 74 and WP 108 as well as the WP 155, which contains a FAQ list on BCRs. This will be updated as needed; last update in February 2017 (rev. 05).

4.5.4 Authorization Procedures

BCR must be approved by the competent supervisory authority in accordance with the consistency mechanism, Article 57(1)(s), Article 47(1) in conjunction with Article 64(1)(f) of the GDPR. The aim is to ensure that European supervisors, on the basis of a common understanding, take a decision that is shared by all and thus contribute to the uniform application of the GDPR.

The German DSAnpUG-EU has stipulated in s. 19(1) BDSG (2018) that the German lead supervisory authority is the authority in whose state the controller or processor has his German headquarter. In line with the requirements of European law, s. 18 BDSG (2018) provides for a definite regulation of the procedure for cooperation between federal and state authorities.

The legislator has put an end to the current practice whereby individual or, in the case of the mutual recognition procedure, three national supervisory authorities, on the basis of their individual understanding, have taken a decision on the legitimacy of the BCR submitted by a group of undertakings. Experience with the often very long approval procedures has led to legal deadlines now being introduced, which will speed up the procedure. In this context, it is also positive that the silence of a supervisory authority involved in the authorization procedure will be considered as consent, Article 64(3) of the GDPR.

If BCR authorised by the supervisory authorities are used as safeguards for third-country transfers, no further approval of a supervisory authority is required, Article 46(2) of the GDPR. In this way, the European legislator has abolished the practice of some supervisory authorities and thus made an active contribution to harmonised data protection application.

4.5.5 Old-BCR

Article 46(5) of the GDPR makes it clear that authorisations by a supervisory authority on the basis of Article 26(2) Directive 96/46/EC shall remain valid until amended. Thus, approved (old) BCR are basically valid after May 25, 2018 and can be used to safeguard international data transfers.

(Old) BCR, however, reflect the data protection situation under application of Directive 95/46/EC or the national data protection laws enacted thereon. Although the content of the rules on the

'Transfer of personal data to third countries'[5] have been adopted by GDPR, there is likely to be a need for a certain amount of adaptation with regard to other issues. If the amended BCR are submitted to the competent supervisory authority, this shall constitute a notification of change in accordance with Article 47(2)(k) of the GDPR and not an application for approval of (new) BCR.

4.6 Codes of Conduct or Certification

The GDPR introduces two new types of appropriate safeguards.

4.6.1 Codes of Conduct

Article 46(2)(e) of the GDPR refers to approved codes of conduct pursuant to Article 40 of the GDPR as appropriate guarantees if they go together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including data subject's rights.

For this purpose, those controllers or processors in the third country shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards according to Article 40(3) of the GDPR. In addition to the codes of conduct approved by the supervisory authorities, an act of the company is therefore required to ensure that safeguards are enforced in the third country for data subjects. Compliance must be legally enforceable for data subjects – effective legal remedies must be available for this purpose (such as judicial remedies and the right to claim damages).

4.6.1.1. Necessity

If one considers the challenges of the existing transfer mechanisms in recent years (Safe Harbour or current standard data protection clauses), it can be stated that it is risky to base a transfer to a third country only on one of the possible legal bases. The European Court of Justice has also made it clear in its judgment on Safe Harbour that there is no guarantee of a transitional period. Theoretically, one legal basis can be declared invalid ad hoc.

5 This is the title of Chapter IV of Directive 95/46/EC.

4.6.1.2 Potential of Implementation

If codes of conduct are considered in the overall structure of existing legal bases, the threshold should not be set too high. In this context, the already high requirements for recognition according to Article 40 of the GDPR should be taken into account.

4.6.1.2.1 Background

Codes of conduct can only be authorised if the supervisory authorities believe that they contribute to the proper application of the GDPR, e.g. by specifying the rules of the GDPR. In addition, codes of conduct must provide that an independent board shall monitor compliance with the rules and those who have adhered to the rules and who ultimately wish to rely on the legal effects of the rules.

This already means that codes of conduct are not an end in themselves. Codes of conduct in the sense of the GDPR are to be understood as a credible and serious supplement to state supervision. The independent governance body must, for example, provide for a complaint procedure. It must also be equipped with options for adequate sanctions and is itself required to report to the data protection supervisory authority. This not only provides the opportunity to intervene in a corrective manner through state supervision. Rather, it also ensures the high quality of this complementary instrument; after all, independent monitoring boards are also subject to substantial fines in the event of inadequate compliance.

4.6.1.2.2 Practical effects

In this regard, the question arises as to what extent the requirements on codes of conduct with regard to the act of implementation in the respective third country must go beyond what is guaranteed, for example, by standard data protection clauses or binding corporate rules. Neither standard data protection clauses nor BCR will be able to resolve any contradictions with the national law of the third country nor, if necessary, to create (legal) remedies.

Although binding corporate rules and standard data protection clauses are agreements approved by the supervisory authorities, they also remain bilateral agreements which do not require an examination mechanism beyond the provisions stipulated in the law.

If one then understands BCR as a special form of codes of conduct, a relatively clear picture arises as to where the concrete potentials of justifying third-country transfers through codes of conduct lie. Based on the requirements of the BCR and standard data protection clauses, the content of the code should not be expected to go beyond these requirements. Rather, it could be argued that even lower requirements are sufficient, since this ‘minus’ would be compensated by the further safeguarding mechanisms of the codes of conduct.

4.6.1.3 Advantages/Opportunities

Codes of conduct offer controllers and processors the opportunity to centralise individual negotiations with the supervisory authority with regard to industries where data transfers are necessary outside the group of undertakings.

Codes of conduct can also serve as a benchmark for minimum standards in the respective industries and thus influence the European-wide interpretation of the GDPR at an early stage and in a relevant manner. Therefore, it cannot be ruled out that competent supervisory authorities may use the (minimum) level laid down in codes of conduct as a reference for examinations.

Codes of conduct can also be declared as generally valid by the EU Commission.

So far, there are no such codes that justify data transfers.

4.6.2 Certification

According to Article 46(2)(f) of the GDPR and Article 42(2) of the GDPR, an approved certification mechanism may also serve as an appropriate safeguard if it is combined with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regard data subject's rights. The same basic conditions apply as for the approved rules of conduct.

4.7 USA: Privacy Shield

On 12 July 2016, the EU Commission formally adopted the 'EU-US Privacy Shield'. The implementation decision came into force immediately after it was sent to the EU Member States. This has created a new framework for the commercial exchange of personal data between the European Union and the United States, following the end of safe harbour. The Privacy Shield is an 'adequacy decision' (C (2016)4176 final) by the EU Commission in accordance with Article 25(6) of Directive 95/46/EC or Article 45 of the GDPR. The EU Commission has thus established that the US guarantees an adequate level of data protection and that personal data from the EU Member States can be transferred to the US without (further) authorization. The prerequisite for this is that the US companies involved in the data exchange comply with certain information and formal requirements, as well as with the data protection principles set out in Annex II of the Privacy Shield Decision. The conclusion of standard contractual clauses is no longer necessary for certified companies.

Note!

Additional processing contract despite Privacy Shield certification: If personal data is transferred from the EU to the US on behalf of a controller in the EU, a (processing) contract must be concluded between the parties irrespective of whether the US company is privacy-certified (see Annex II, Supplementary Principles III No. 10 'Obligatory Contracts for Onward Transfers'). For readers (still) focused on the BDSG, this requirement may feel wrong, as s. 3 No. 8 BDSG did not allow a processing contract with a company in a third country. However, if we look at Directive 95/46/EC and especially the GDPR, this requirement fits logically. Due to the extension of the territorial scope to processing and controllers outside of the European Union (Article 3 of the GDPR), processing on behalf of the controller outside the EU will also be possible in the future. For processing on behalf in the United States, the authors of the Privacy Shield decision have explicitly stated that in this case, a processing contract must be concluded, which contains the following points:

- processors act only on instructions from the controller,
- processors ensure appropriate technical and organizational measures,
- processors assist the controller with regard to the rights of the data subject (of importance due to Art. 13(1)(f) of the GDPR).

The decision to join the Privacy Shield is entirely voluntary – effective compliance with the principles is mandatory.

US companies have been able to join the Privacy Shield since August 1, 2016. Currently, 2509 companies are registered (status 11.10.2017). The list is publicly accessible ↗website (https://www.privacyshield.gov/list). The U. S. Department of Commerce (FTC) issues the certificates after the company has provided all the necessary information for the certification process (self-certifying). The certification shall be renewed annually (see Annex II, Overview I, No. 3). In the event that the company does not renew its certification after one year, the FTC deletes the company from the list. The company will then be listed in the Privacy Shield list as 'inactive' (on October 11,2017,31 companies were listed as 'inactive'?.

The regulatory content of the Privacy Shield is set out in Annex II of the Privacy Decision. Under (I) in the 'Overview' the motivation for the common data exchange is described, as well as the general duties. (II) establishes 'principles' which serve to protect the data subjects. This includes, among other things, information on participation in the Privacy Shield, the possibility of objecting to data disclosure (opt-out), the right to information and legal protection. (III) describes 'Supplemental principles' relating to business processes, such as journalistic exceptions, due diligence and auditing, the role of the data protection authority, audits and complaints procedures.

Due to an Executive Order of President Trump dated January 25, 2017, voices were raised that questioned the continued existence of the Privacy Shield. In an answer to a parliamentary question by the European Parliament on 5 April 2017, EU Commissioner Jourová states that the US Department of Justice officially confirms in an answer that Section 14 of the Executive Order does not affect the obligations under the Privacy Shield. For the time being, the Privacy Shield will serve as a basis for transatlantic data exchange.

It should also be noted that the French consumer protection organization La Quadrature du Net (Case T-738/16) and the Irish NGO Digital Rights Ireland (Case T-738/16) have filed separate EU lawsuits against the EU Commission's Privacy Shield. Before the CJEU can deal with the Privacy Shield in these proceedings, it must first be clarified whether the two parties, as non-governmental organizations, are entitled to sue under EU-law. This decision is still pending.

Irrespective of this, the United States and the European Union carried out the first review of the Privacy Shield together in September 2017. On the whole, the report showed that the Privacy Shield continues to ensure an adequate level of data protection. However, recommendations were made to improve the functioning of the Privacy Shield. More information by the EU Commission can be found ↗here.

For more information, see:

↗Press Releases
↗Decision on adequacy ((EU)2016/1250 of 12 July 2016)
↗Appendix/Annexes
↗FAQ
↗fact sheet
↗Announcement by Mrs. Jourová on the Executive Order

The European Commission has published a ↗guide to explain the remedies available to EU citizens in cases of breaches of data protection.

The Bavarian State Office for Data Protection Supervision has also ↗published an overview of the Privacy Shield and a complaint form for citizens.

5 Intra-group Data Transfers

5 Intra-group Data Transfers

5.1 General Information

Unlike, for example, in tax and corporate law, there has not been and still is no privilege for corporate groups in data protection law. The legitimacy of processing personal data must be checked individually by each individual legal entity of the group in accordance with the provisions of the GDPR – provided they are applicable.

However, if some aspects of the processing of employee and customer data are discussed in the following, it is because there is sometimes legal uncertainty in this respect or they may deviate from previous practice. It makes no difference whether the processing is carried out internally or externally, nationally or internationally.

5.2 Principles of Processing Personal Data

The principles of the processing of personal data are laid down in Article 5(1) of the GDPR. This includes the principle of transparency, according to which processing must be carried out in a transparent manner in relation to the data subject. For data processing in the context of employment, Member States may lay down 'more specific' regulations in accordance with Article 88 of the GDPR. It remains to be seen whether and how Germany will make use of this national opening clause, for example through an employment data protection law that is repeatedly being discussed. To date, there is only a brief statement on transparency requirements in s. 26(4) BDSG (2018). They are dealt with in the context of works agreements (under 6.3.4).

5.3 Legality of Processing

A processing of personal data of employees and customers is only allowed if it is based on one of conclusive legal bases listed in Article 6(1) of the GDPR. There are certain special characteristics of the following three legal bases.

5.3.1 Consent

Data processing is lawful if the data subject has given effective consent. According to Article 4 No. 11 of the GDPR, consent is any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies the agreement to the processing of personal data relating to him or her.

The requirement of 'freely given' may be not fulfilled if there is a clear imbalance between the data subject and the controller, Recital 43 of the GDPR. The EU Commission's proposal for the GDPR still contained the statement that such an imbalance exists in specifically in employment

relations. By deleting this reference, it is made clear that consent is also principally possible in the employment relationship.[6]

In which cases the consent of an employee is freely given and thus effective is one of the regulatory questions which, according to Article 88 of the GDPR can be regulated 'more specifically' by the Member States, Recital 155 GDPR. Germany has made use of this national opening clause with the adoption of the DSAnpUG-EU. In s. 26(2) BDSG (2018) it lays down criteria which must be taken into account when determining the voluntary nature of consent, for example, the individual dependency and the circumstances in which the consent is given. S. 26(2) sentence 2 BDSG (2018) mentions the legal or economic advantageousness for the employee as indication to determine whether the consent is freely given. Whether and to what extent the 'Opinion on data processing at work' of the WP29 can be used to interpret the nature of freely given consent in employment law under national legislation, is questionable. On the one hand, national law specifies clear criteria that allow little room for interpretation and, on the other hand, the opinion of the European supervisory authorities is considerably more restrictive than the new legislation in Germany, as they always have to take into account the respective national labour law conditions.

Pursuant to s. 26 (2) Sentence 3 BDSG (2018), consent must be given in writing. Whether this legal requirement can be based on the employer's general documentation duty (according to the legal justification) or whether the German legislator has exceeded the scope of opening clauses in Article 88 of the GDPR, the courts will have to clarify in case of doubt. Either way, the employer must be able to prove that he has informed the employee comprehensively, namely in text form (s. 26 (2) sentence 4 BDSG (2018)) and has received consent relating to the specified processing.

5.3.2 Performance of a Contract

Processing of personal data of employees of a group of company can be legitimised according to Article 6(1)(b) of the GDPR. With s. 26(1) BDSG (2018), the German legislator has introduced a more specific provision based on the opening clause of Article 88(1) of the GDPR. Accordingly, personal data of employees may be processed for the purposes of employment if this is necessary for deciding on the establishment of an employment relationship or for the exercise or termination of the employment relationship. By splitting up the definition of employment relationship, the German legislator merely exemplified what this means in any case, making use of the familiar terminology of s. 32 BDSG (2009). This does not mean, however, that other processing of personal data of employees that are required for the fulfilment of the employment relationship would not be allowed. Such a restriction on legal bases would not be allowed under EU law.[7] Thankfully, the German legislator has made it clear in s. 26(8) BDSG (2018) that the term employee needs to be understood comprehensively under data protection law.

6 See also WP29 in its Opinion 2/2017 on data processing at work (WP 249).

7 CJEU, Decision of 24/11/2011, ASNEF and FECEMD, C-468/10 and C-469/10.

5.3.3 Legitimate Interest

In practice, the processing of personal data is often legitimised by reference to the safeguarding of legitimate interests. The meaning of 'legitimate interests' in the sense of Article 6(1)(f) of the GDPR and when they are likely to outweigh the interests or rights of the data subject, has been explained by the European supervisory authorities in their 'Opinion on the concept of the legitimate interests of the controller' (WP217).

In the case of data processing in the context of an employment relationship, there is no doubt that the legal basis of legitimate interest is applicable. This is clearly stated in the Recital 48[8] which clarifies that the transmission of employee's or client's data to other affiliates of a group of undertakings for internal administrative purposes can be considered as legitimate interest.

Some consider this as a kind of 'small group privilege'. This is not true, as it is not a matter of improving or privileging intra-group transfers over other types of processing. Recital 48 of the GDPR does not regulate anything new, but merely mentions as an example that for the constellations listed, a transmission can be carried out if there are legitimate interests. The GDPR has copy-pasted the legal basis of legitimate interest from Directive 95/46/EC. In contrast to many other Member States, however, the German implementation neither followed the wording nor the system of Article 7 of Directive 95/46/EC but only made a few adjustments to the BDSG (1990) which do not really reflect the core of the European law. This explains why in other Member States the legitimacy of intra-group transfers was not considered as problem and why the European legislator saw no need to introduce a provision in the sense of a group privilege. Therefore, all well-intentioned proposals of the European Parliament were doomed to fail. However, the European legislator felt compelled to clarify this matter in a Recital in order to ensure the harmonised application of the legitimate interest legal basis.

The European data protection authorities see the establishment of a company-wide internal employee database with contact data, as a further example of which intra-group transfers can be justified by the protection of legitimate interests, WP 217, p. 22.

Practical Advice!

If the controller uses the legal basis of legitimate interest, he or she should document this in relation to the specific processing activity. Otherwise, he can neither fulfil his duty of accountability under Article 5(2) of the GDPR nor his or her obligation to provide information to the data subject (Article 13(1)(d), Article 14(2)(b), Article 21(1) of the GDPR).

8 In the opinion of the European supervisory authorities organised in the Working Party on Data Protection, this permission can also be applied in the context of an employment relationship, e. g. see WP 217 and WP 247.

5.3.4 Works Agreements

The GDPR has clarified in Recital 155 that more 'specific rules on the processing of employee's personal data in the employment context' in collective agreements including works agreements can be laid down according in line with Article 88 of the GDPR. However, these do not constitute separate legal bases for processing data, but merely serve to further adapt the data processing of employees, legitimised on basis of Article 6(1) of the GDPR, to the situation of the individual company. The legislator thereby set forth the findings of the European Court of Justice[9] on the possibility of changing legal grounds under Article 6(1) of the GDPR, according to which the Member States may not amend them in any way, either by extending or restricting them.

In s. 26(4) sentence 1 BDSG (2018) the German legislator repeats the statement of the GDPR, according to which in collective agreements, employment relationships can be structured in accordance with data protection requirements. According to the legal justification, this also includes company and service agreements. The second sentence of this paragraph refers to Article 88(2) of the GDPR, according to which such agreements 'shall in particular ensure the transparency of processing'. That means that collective and works agreements must be easily accessible to employees. If the wording of a works agreement is worded in such a way that an average employee cannot undoubtedly identify the purposes for which his or her personal data are to be processed, a generally understandable summary must also be attached. Otherwise, the legal obligation to use 'a clear and simple language' (according to Article 12 of the GDPR) is not complied with.

5.4 Data Processing on Behalf by Affiliates

As a result of the general tendency to centralize processes, it is becoming increasingly common within a group of undertakings that individual affiliates provide services for other affiliates such as accounting, payroll, recruiting, etc.

5.4.1 Contract for Data Processing on Behalf

Insofar as personal data is processed on behalf, the affiliates of a group have to conclude a contract pursuant to Article 28 of the GDPR for the respective intra-group transfers.

9 CJEU, Decision from 24/11/2011 (ASNEF) and (FECEMD), C-468/10 and C-469/10.

Practical Advice!

In order to avoid that all commissioning affiliates of a group enter into individual contracts with the one commissioned affiliate in accordance with Article 28 of the GDPR, one can also choose the following solution: The parent company (controller within the meaning of Article 4 No. 7 of the GDPR) concludes a contract with the commissioned affiliate (processor within the meaning of Article 4 No. 8 of the GDPR) in accordance with Article 28 of the GDPR, to which the other affiliates of the group are joining (as controllers). Accession must be documented, i. e. verifiable, in order for the affiliates to fulfil the accountability requirements.

5.4.2 In Writing

The contract for data processing on behalf of a controller must be in writing. This does not mean, however, according to the European understanding, that the validity of the contract requires the personal signature of the contracting parties. 'Written' as laid down in Article 28(9) of the GDPR is to be understood in the sense of 'documented', for which an electronic format is sufficient. The partly dissenting opinion in Germany, according to which 'written' is to be understood as a mandatory written form requirement within the meaning of s. 126 BGB, can therefore no longer be maintained. However, it should be borne in mind that affiliates of group have to comply with their duty of accountability. They can also fulfil this obligation by signing the contract for data processing on behalf as annex to the service agreement, which is advisable in case of the inclusion of non-Group external partners.

5.4.3 Legitimacy without 'Data Processing on Behalf'

The German data protection law has differentiated in the case of data processing on behalf ('Auftrags(daten)verarbeitung' as the usual designation in Germany) as follows: If data is processed on behalf of a service provider (data processor) within the European Economic Area (EEA), the data transfer is a transmission which does not need a specific legitimation. By contrast, in the exercise of the same activity, the service provider outside the EEA is a third party and data transfer requires legitimisation, which is seen by a majority in the 'safeguarding of legitimate interests' within the meaning of s. 28 (1) No. 2 BDSG (2001).[10]

This differentiation is unknown to the European data protection law of Directive 95/46/EC or the GDPR. The service provider who processes personal data on behalf of controller is always a processor, irrespective of the place of processing (Article 4(8) of the GDPR). The data transfer to the processor is always a transmission and thus a 'processing' in the sense of European law (Article 4(2) of the GDPR). The necessary legitimacy for the transfer to the processor, but also all other processing operations in this context, can be deduced from the role of the controller and

10 More information in Drewes/Monreal in PinG 2014, p. 143ff.

his or her legally assigned role. There is therefore no need for any further or special legal basis. The characteristic criterion of the controller is his authority to determine the purposes and means of processing. If a controller is processing data on the basis of a legal basis laid down in Article 6 of the GDPR, he can freely decide whether the processing of data is carried out – wholly or partly – by himself or engages a processor who processes data on behalf of him or her for which a transmission of data could be necessary.

5.5 Joint Controllers

According to the GDPR, two or more controllers can jointly determine the purposes and means of processing, Article 4(7) of the GDPR. In such a case, the concerned affiliates of a group must conclude a transparent agreement that complies with the requirements of Article 26 of the GDPR. Where an affiliate of a joint controllers is established in a third country without adequate protection, 'appropriate safeguards', e. g. in the form of BCR, are also required.

6 Definitions, Material, Graphics and Overviews

6 Definitions, Material, Graphics and Overviews

6.1 Definitions

The following is a brief explanation of some key data protection terms:

- **Data Processing on Behalf of a Controller/Data Processor**
  Data processing on behalf of the controller is a data processing of personal data by the processor (supplier) according to instructions and on behalf of the controller (company). A processor is a natural or legal person who processes persona, data on behalf of the controller, see Article 4 No. 8 of the GDPR.

- **Processing of Special Categories of Personal Data**
  A distinction must be made between the general personal data and the specific categories of data. These are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex or sexual orientation; see Article 9 of the GDPR.

- **Data Subject**
  Any natural person whose privacy is at issue and who is to be protected from being affected by the processing in his right to protection of personal data; see Article 4 No. 1 of the GDPR.

- **Data Exporter**
  The data exporter is the controller who transfers personal data.

- **Data Importer**
  The data importer is the controller who agrees to receive personal data for processing from the data exporter.

- **Third Party**
  A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data (Article 4 No. 10 of the GDPR). The term 'third party' does not include legally dependent branches of a company. Legally independent institutions – such as company health insurance funds – are, however, also third parties if they are linked organizationally, spatially or through personnel to the controller or processor.

- **Third Country**
  Third countries are all other countries outside the EU (more info on EEA see 2.1).

- **Consent**
  Any freely given, specific, informed and unambiguous indication of the data subjects wishes by

which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her; Article 4 No. 11 of the GDPR.

- **Recipient**
  Recipient is every entity receiving data.

- **Personal Data**
  Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier (e.g. IP address or cookie identifier) or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity or that natural person; see Article 4 No. 1 of the GDPR. Legal persons under private law (e.g. GmbH, BV, LTD) are not covered by this.

- **Enterprise**
  A natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity; see Article 4 No. 18 of the GDPR. This means that the concept of enterprise in data protection is very broad and encompasses every company regardless of size and industry, so that freelancers, for example, are also covered.

- **Group of Undertakings**
  A controlling undertaking and its controlled undertakings; see Article 4 No. 19 of the GDPR and Article 37, 47 and 88 of the GDPR where definitions play a role. The definition is limited to a group of undertakings where an undertaking can exercise a controlling influence over the other undertakings, e. g. due to ownership, financial participation or the rules applicable to the enterprise or the authority to have data protection regulations implemented (Recital 37 of the GDPR). Other definitions, such as a group of undertakings which carry on a joint economic activity and which are not covered by the concept of self-employment, are to be distinguished from it.

- **Processing of Personal Data**
  Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destructions; Article 4 No. 2 of the GDPR.

- **Binding Corporate Rules**
  Personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity; see Article 4 No. 20 of the GDPR.

- **Controller**
  Natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing of personal data; see Article 4 No. 7 GDPR.

- **Representative**
  A natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27 of the GDPR, represents the controller or processor with regard to their respective obligations under this Regulation; see Article 4 No. 17 of the GDPR. This definition is only relevant for controllers or processors that are not based in the EU.

6.2 EU-US Privacy Shield Materials

6.2.1 The Privacy Shield Principles

Notice

An organization must inform individuals about:

- its participation in the Privacy Shield and provide a link to, or the web address for, the Privacy Shield List,
- the types of personal data collected and, where applicable, the entities or subsidiaries of the organization also adhering to the Principles,
- its commitment to subject to the Principles all personal data received from the EU in reliance on the Privacy Shield,
- the purposes for which it collects and uses personal information about them,
- how to contact the organization with any inquiries or complaints, including any relevant establishment in the EU that can respond to such inquiries or complaints,
- the type or identity of third parties to which it discloses personal information, and the purposes for which it does so,
- the right of individuals to access their personal data,
- the choices and means the organization offers individuals for limiting the use and disclosure of their personal data,
- the independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to the individual, and whether it is: (1) the panel established by DPAs, (2) an alternative dispute resolution provider based in the EU, or (3) an alternative dispute resolution provider based in the United States,

- being subject to the investigatory and enforcement powers of the FTC, the Department of Transportation or any other U.S. authorized statutory body,
- the possibility, under certain conditions, for the individual to invoke binding arbitration,
- the requirement to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements, and
- its liability in cases of onward transfers to third parties.

This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.

Choice

I. An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (i) to be disclosed to a third party or (ii) to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individuals. Individuals must be provided with clear, conspicuous, and readily available mechanisms to exercise choice.

II. By derogation to the previous paragraph, it is not necessary to provide choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. However, an organization shall always enter into a contract with the agent.

III. For sensitive information (i.e., personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), organizations must obtain affirmative express consent (opt in) from individuals if such information is to be (i) disclosed to a third party or (ii) used for a purpose other than those for which it was originally collected or subsequently authorized by the individuals through the exercise of opt-in choice. In addition, an organization should treat as sensitive any personal information received from a third party where the third party identifies and treats it as sensitive.

Accountability for Onward Transfer

I. To transfer personal information to a third party acting as a controller, organizations must comply with the Notice and Choice Principles. Organizations must also enter into a contract with the third-party controller that provides that such data may only be processed for limi-

ted and specified purposes consistent with the consent provided by the individual and that the recipient will provide the same level of protection as the Principles and will notify the organization if it makes a determination that it can no longer meet this obligation. The contract shall provide that when such a determination is made the third party controller ceases processing or takes other reasonable and appropriate steps to remediate.

II. To transfer personal data to a third party acting as an agent, organizations must: (i) transfer such data only for limited and specified purposes; (ii) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Principles; (iv) require the agent to notify the organization if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles; (v) upon notice, including under (iv), take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vi) provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request.

Security

Organizations creating, maintaining, using or disseminating personal information must take reasonable and appropriate measures to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.

Data Integrity and Purpose Limitation

I. Consistent with the Principles, personal information must be limited to the information that is relevant for the purposes of processing.[11] An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization must take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete, and current. An organization must adhere to the Principles for as long as it retains such information.

11 Depending on the circumstances, examples of compatible processing purposes may include those that reasonably serve customer relations, compliance and legal considerations, auditing, security and fraud prevention, preserving or defending the organization's legal rights, or other purposes consistent with the expectations of a reasonable person given the context of the collection.

II. Information may be retained in a form identifying[12] or making identifiable the individual only for as long as it serves a purpose of processing within the meaning of 5a. This obligation does not prevent organizations from processing personal information for longer periods for the time and to the extent such processing reasonably serves the purposes of archiving in the public interest, journalism, literature and art, scientific or historical research, and statistical analysis. In these cases, such processing shall be subject to the other Principles and provisions of the Framework. Organizations should take reasonable and appropriate measures in complying with this provision.

Access

Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the Principles, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

Recourse, Enforcement and Liability

Effective privacy protection must include robust mechanisms for assuring compliance with the Principles, recourse for individuals who are affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum such mechanisms must include:

I. readily available independent recourse mechanisms by which each individual's complaints and disputes are investigated and expeditiously resolved at no cost to the individual and by reference to the Principles, and damages awarded where the applicable law or private-sector initiatives so provide;

II. follow-up procedures for verifying that the attestations and assertions organizations make about their privacy practices are true and that privacy practices have been implemented as presented and, in particular, with regard to cases of non-compliance; and

III. obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.

Organizations and their selected independent recourse mechanisms will respond promptly to inquiries and requests by the Department for information relating to the Privacy Shield. All

12 In this context, if, given the means of identification reasonably likely to be used (considering, among other things, the costs of and the amount of time required for identification and the available technology at the time of the processing) and the form in which the data is retained, an individual could reasonably be identified by the organization, or a third party if it would have access to the data, then the individual is ´identifiable.´

organizations must respond expeditiously to complaints regarding compliance with the Principles referred by EU Member State authorities through the Department. Organizations that have chosen to cooperate with DPAs, including organizations that process human resources data, must respond directly to such authorities with regard to the investigation and resolution of complaints.

Organizations are obligated to arbitrate claims and follow the terms as set forth in Annex I, provided that an individual has invoked binding arbitration by delivering notice to the organization at issue and following the procedures and subject to conditions set forth in Annex I.

In the context of an onward transfer, a Privacy Shield organization has responsibility for the processing of personal information it receives under the Privacy Shield and subsequently transfers to a third party acting as an agent on its behalf. The Privacy Shield organization shall remain liable under the Principles if its agent processes such personal information in a manner inconsistent with the Principles, unless the organization proves that it is not responsible for the event giving rise to the damage.

When an organization becomes subject to an FTC or court order based on non-compliance, the organization shall make public any relevant Privacy Shield-related sections of any compliance or assessment report submitted to the FTC, to the extent consistent with confidentiality requirements. The Department has established a dedicated point of contact for DPAs for any problems of compliance by Privacy Shield organizations. The FTC will give priority consideration to referrals of non-compliance with the Principles from the Department and EU Member State authorities, and will exchange information regarding referrals with the referring state authorities on a timely basis, subject to existing confidentiality restrictions.

6.2.2 Privacy Shield Supplemental Principles

1. Sensitive Data
2. Journalistic Exceptions
3. Secondary Liability
4. Performing Due Diligence and Conducting Audits
5. The Role of Data Protection Authorities
6. Access
7. Self-Certification
8. Verification
9. Human Resources Data
10. Obligatory Contracts for Onward Transfers
11. Dispute Resolution and Enforcement
12. Choice – Timing of Opt-Out
13. Travel information
14. Pharmaceutical and Medical Products
15. Public Record and Publicly available Information
16. Access Requests by Public Authorities

More information can be found in the Commission's ↗Adequacy Decision and Annexes (see Annex II).

6.2.3 Overview EU Commission Fact Sheet

Strong obligations on companies and robust enforcement

- Greater transparency
- Oversight mechanisms to ensure companies abide by the rules
- Sanctions or exclusion of companies if they do not comply
- Tightened conditions for onward transfer

Redress

Several redress possibilities

- Directly with the company: Companies must reply to complaints from individuals within 45 days.
- Alternative Dispute Resolution: Free of charge
- With the Data Protection Authority: They will work with U.S. Department of Commerce and Federal Trade Commission to ensure unresolved complaints by the EU citizens are investigated and swiftly resolved.
- Privacy Shield Panel: As a last resort, there will be an arbitration mechanism to ensure an enforceable decision.

U.S. Government access

- For the first time, written assurance from the U.S. that any access of public authorities to personal data will be subject to clear limitations, safeguards, and oversight mechanisms.
- U.S. authorities affirm absence of indiscriminate or mass surveillance.
- Companies will be able to report approximate number of access requests.
- New redress possibility through EU-U.S. Privacy Shield Ombudsperson mechanism, independent from the intelligence community, handling and solving complaints from individuals.

Monitoring

Annual joint review mechanism:

- Monitoring the functioning of the Privacy Shield and U.S. commitments, including as regards access to data for law enforcement and national security purposes.
- Conducted by the European Commission and the U.S. Department of Commerce, associating national intelligence experts from the U.S. and European Data Protection Authorities.

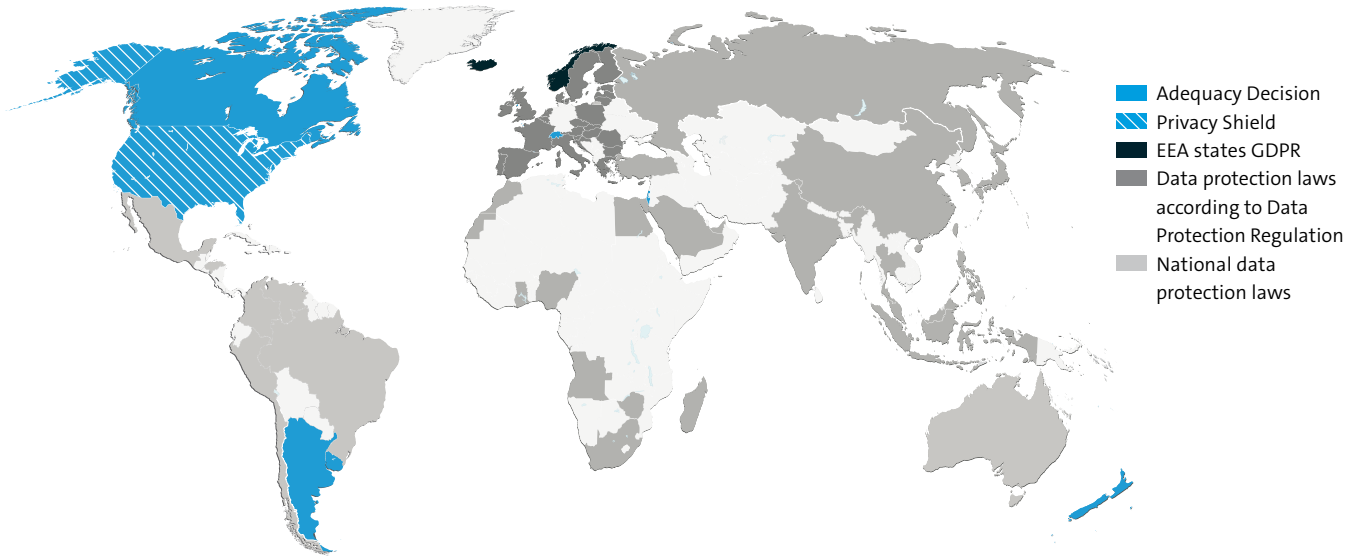
Source: ↗Fact sheet of EU Commission (2016)

6.3 Overview of Status of Global Data Protection

6.3.1 Graphic Overview of Worldwide Data Protection Status

Notice: According to the EU Commission more and more countries around the world have adopted new legislation on data protection in recent years or are in the process of doing so. In 2015, the number of countries that had enacted privacy laws stood at 109, a significant increase from 76 in mid-2011, ↗EU-Communication (2017) 7, p. 7. In 2017, this number has increased by another 10 % to 120 countries.[13]

An overview of national data protection laws can we also found on the ↗website of DLA Piper.



13 Greenleaf, Graham, Global data privacy laws (5th edition 2017), status 30 June 2017.

6.3.2 Explanation of the Graphical Overview of the Worldwide Status of Data Protection

Status October 2017

Data protection laws according to the General Data Protection Regulation	EEA States
Belgium	Iceland
Bulgaria	Liechtenstein
Denmark	Norway
Estonia	
Finland	
France	
Greece	
Great Britain	
Ireland	
Italy	
Croatia	
Latvia	
Lithuania	
Luxembourg	
Malta	
Netherlands	
Austria	
Poland	
Portugal	
Romania	
Sweden	
Slovakia	
Slovenia	
Spain	
Czech Republic	
Hungary	
Cyprus	

Adequate data protection level recognised by EU Commission	EU-U.S. Privacy Shield
Argentina	USA
Andorra	
Guernsey	
Isle of Man	
Jersey	
Canada	
New Zealand	
Israel	
Switzerland	
Faeroe islands	
Uruguay	

Data Protection Authorities in Europa (outside EEA)	Data Protection Authorities International	
Albania	Antigua and Barbuda	Mexico
Armenia	Argentina	Nepal
Bosnia and Herzegovina	Australia	New Zealand
Georgia	Bahamas	Paraguay
Kosovo	Benin	Peru
Macedonia	Brazil	Philippine
Moldavia	Burkina Faso	São Tomé and Príncipe
Montenegro	Chile	Senegal
Russia	Costa Rica	Zimbabwe
Switzerland	Dom. Rep.	Singapore
Serbia	Dubai	South Africa
Turkey	Ivory Coast	South Korea
Ukraine	Equatorial Guinea	Senegal
	Gabon	St. Lucia
	Hong Kong	Taiwan
	Israel	Thailand
	Japan	Trinidad and Tobago
	Yemen	Tunisia
	Hong Kong	Uruguay
	Canada	USA
	Kap Verde	
	Kazakhstan	
	Kyrgyzstan	
	Columbia	
	Lesotho	
	Costa Rica	
	Macao	
	Malaysia	
	Malawi	
	Mali	
	Marokko	
	Mauritius	

Source: International Conference of Data Protection & Privacy Commissioners (↗ICDPPC). Greenleaf gives also a good overview in Global Tables of data Privacy Laws and Bills (5th edition 2017).

National Data Protection Laws[14]	
Abu Dhabi (2015)	Moldawien (2007)
Albania (1999/2012)	Montenegro (1998/2008)
Angola (2011)	Nepal (2007)
Antigua & Barbuda (2013)	New Zealand (1993/2010)
Argentina (2000)	Nicaragua (2012)
Armenia (2002/2015)	Norway (1978/2010)
Equatorial Guinea (2016)	Paraguay (2002)
Aruba (2011)	Peru (2011)
Australia (1988/2012)	Philippine (2012)
Azerbaijan (1998/2010)	Russia (2006/2011 und 2014)
Benin (2009)	São Tomé and Príncipe (2016)
Bahamas (2003)	Switzerland (1992/2006)
Bermuda (2016)	Senegal (2008)
Bosnia and Herzegovina (2001)	Serbia (2008)
Burkina Faso (2004)	Seychelles (2003)
Chad (2015)	Zimbabwe (2002)
Chile (1999/2012)	Singapore (2012)
Costa Rica (2011/2013)	St. Lucia (2011)
Curacao (2010)	St. Maartens (2010)
Dominican Republic (2013)	St. Vincent & Grenadines (2003)
Dubai (2007)	South Africa (2013)
Ivory Coast (2013)	South Korea (1994/2015)
Equatorial Guinea (2016)	Taiwan (1995/2010)
Gabon (2011)	Thailand (1997)
Georgia (2012)	Trinidad and Tobago (2011)
Ghana (2012)	Tschad (2015)
Hong Kong (1995/2012)	Tunisia (2004)
India (2011)	Ukraine (2011/2015)
Indonesia (2016)	Uruguay (2008)
Israel (1981)	Vietnam (2010)
Japan (2003/2015)	United States (1994)
Jemen (2012)	
Canada (1983/2002)	
Cape Verde (2001)	
Caribbean Netherlands (2010)	
Kasachstan (2013/2015)	
Katar (2016)	
Kirgistan (2008)	
Kolumbien (2008/2012)	
Kosovo (2010)	
Lesotho (2011)	
Macao (2006)	
Madagaskar (2015)	
Malawi (2016)	
Malaysia (2010/2013)	
Mali (2013)	
Marokko (2009)	
Mauritius (2004)	
Mazedonien(1994/2005)	
Mexiko (2010/2016)	

Notice: Only the countries that have enacted a data protection act are listed here. This does not mean that there are no data protection regulations in the other countries.

14 Greenleaf, Graham, Global data privacy laws (5th edition 2017) Status 30 June 2017.

6.4 Overview of the Legal Possibilities for Data Transfer to Third Countries

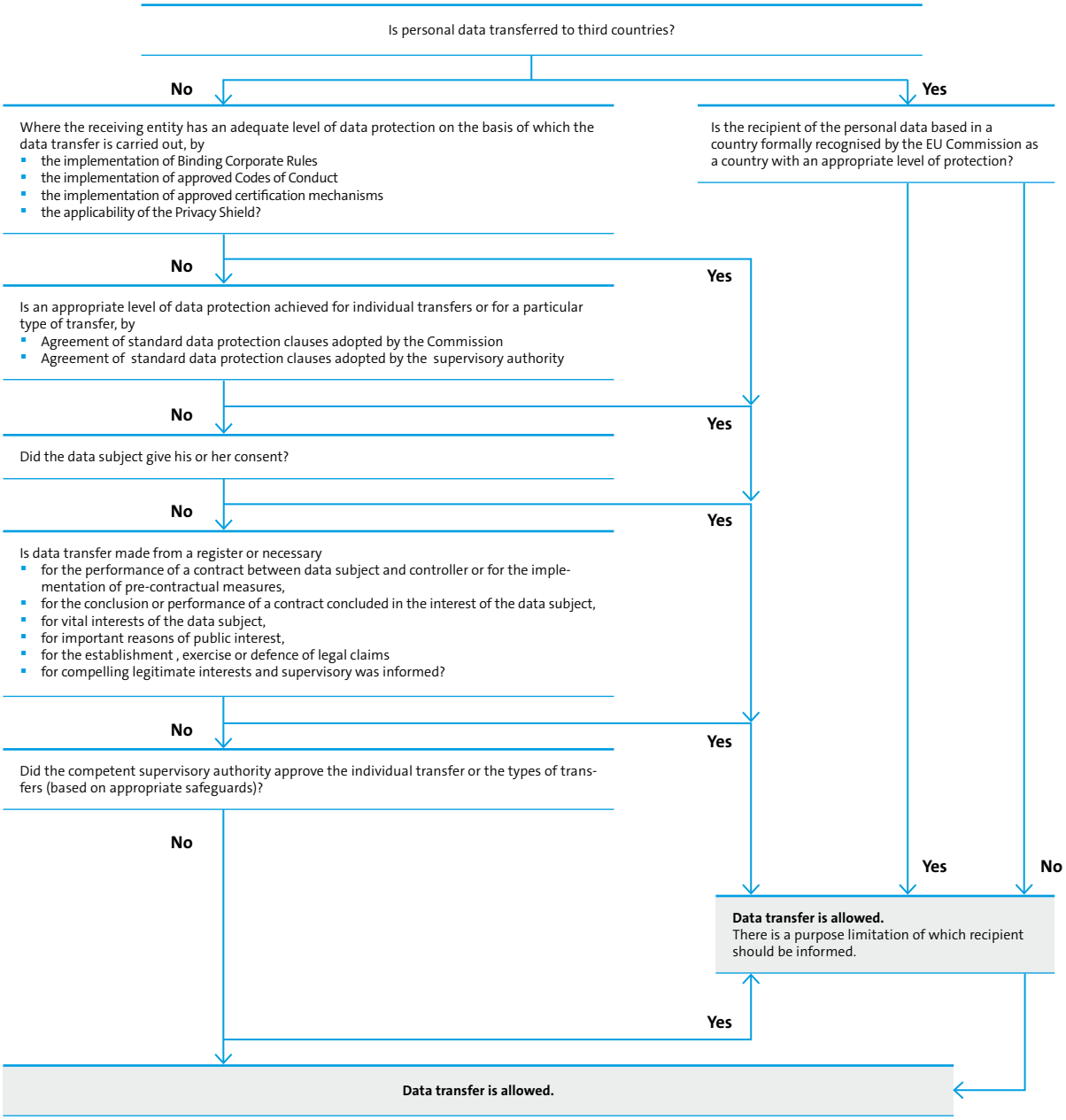
	'Type'	Scope	Conclusion	Personal Data	Supvisory Authority	Comment
Consent (Article 49 (1)(a))	Unilateral declaration needing receipt	Individual; between the data subject and the controller	By submitting the corresponding declaration of intent of the consenting party	Basically the authorised personal data of the data subject; scope within the limits of the legal possibilities, intended purpose	No cooperation required	The data subject must have been informed of possible risks for him/her and must have given his/her explicit consent
Transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures (Article 49(1)(b))	Contract or quasi-contractual relationship between the controller and the data subject	Individual; between the data subject and the controller	By submitting the corresponding declarations of intent from the controller and the data subject	Basically the personal data of the data subject, which is necessary for the execution of the contract	No cooperation required	Examples of contracts: Hotel reservation abroad; employment contract with foreign employer; order of goods (also online) abroad
Data transfer is necessary for the performance of a contract concluded in the interest of the data subject (Article 49 (1)(c))	Contract between the controller and a third party	Individual; between the controller and a third party	By submitting the corresponding declarations of intent from controller and third party	Basically the personal data of the concerend data subject, which is necessary for the execution of the contract	No cooperation required	Sample contracts: Transfer of employee data for employee insurance to foreign insurance company
Other derogations (Article 49 (1)(d)-(f))	Other derogations	Limited to specific situation of derogation	Check whether the legal requirements for the exception are met	Employees, customers, non-customers, interested parties and supplier data, insofar as this is necessary for transfer within the scope of the derogation	No cooperation required	e.g. necessary for important reasons of public interests; the establishment, exercise or defence of legal claims; necessary to protect vital interests of data subject
Third countries with adequacy decision by the EU Commission (Article 45)	Decision according to Article 45 (adequacy decision)	Applies to all recipients in the third country of the decision	n.a.	Employee, customer, non-customer, prospect and supplier data	No cooperation required	Commission Decisions so far: Argentina, Andorra, Guernsey, Isle of Man, Jersey, Canada, New Zealand, Israel, Switzerland, Faroe Islands, Uruguay

	'Type'	Scope	Conclusion	Personal Data	Supvisory Authority	Comment
Individual Contractual Clauses (Article 46 (3)(a))	Contractual, binding regulation between the parties (including several sub-processors) on the handling of personal data	Between the contracting parties (also more than 2) e. g. data exporter (controller processor) and data importer (controller, processor)	By submitting the corresponding declarations of intent between the contracting parties	Employee, customer, non-customer, prospective customer and supplier data as long as they are to be the subject of the individual data protection agreement	Approval of individual data transfers or certain types of transfers of personal data by the supervisory authority in accordance with Article 46 (3)	Flexible; (e. g. adaptation to the specific characteristics of a particular industry); depending on scope, time-consuming; Essential data protection safeguards of the GDPR as well as enforceable rights and effective legal remedies for the persons
Contract on basis of standard data protection clauses (also for data processors) (Article 46 (2) (c)-(d))	Contract between data exporter and data importer on the basis of the EU Commission's decision on the standard data protection clauses or approved standard data protection clauses of the supervisory authorities	Between data importer (s) in a third country and exporter (s) established in the EU	By submitting the corresponding declaration of intent between the contracting parties	Employee, customer, non-customer, prospective customer and supplier data as long as they are to be the subject of the individual data protection agreement	No approval required for unchanged conclusion of the contract	Quickly implemented. Simple. Unfeasible for large international corporate groups, since extensive contract management is required
Binding Corporate Rules (Article 46 (2)(b) and Article 47)	Binding Corporate Rules for parts or all of a multinational group of undertakings (Group) or companies carrying out a joint economic activity (e. g. certain industries)	The parts of the group for which BCR are binding	Binding, internal instruction by the leading company	Employee, customer, non-customer, prospective customer and supplier data as long as they are to be the subject of the individual data protection agreement	No (additional) further regulatory approvals required after completion	
Approved Codes of Conduct (Article 46 (2)(e))	Agreement controllers or processors on approved codes of conduct for data protection	Data transfer of personal data between data exporters established in the EU and companies participating in Code of Conduct (data importer)	Companies' accession to the Code of Conduct through a legally binding and enforceable obligation to comply with the safeguards contained in the rules of the CoC.	Employee, customer, non-customer, prospective customer and supplier data within the scope of registration	No further approvals required after approval of the competent supervisory authority and validation by the EU Commission	

	'Type'	Scope	Conclusion	Personal Data	Supvisory Authority	Comment
Approved certification mechanism (Article 46 (2)(f) and Article42)	Legally binding and enforceable obligations to comply with appropriate safeguards by the controller or processor	Data transfer personal data between data exporters established in the EU and companies certified by certification bodies or supervisory authorities (data importer)	Data exporters and importers were classified in accordance with certification criteria laid down by the certification bodies or by the competent supervisory authority	Employee, customer, non-customer, prospective customer and supplier data within the scope of registration	No further approvals required after certification	
Privacy Shield	Agreement between the US and the EU on binding rules data protection rules for US companies	Data traffic of personal data between data exporters based in the EU and companies participating in Privacy Shield (data importer) in the US	Accession of US companies to the Privacy Shield Programme by declaration of accession, registration on an Internet website and publication of certain information; data exporter must be established in the EU	Employee, customer, non-customer, prospective customer and supplier data within the scope of registration	No cooperation required; if necessary, the company that wants to transfer data must inform the recipient of his/her participation in the Privacy Shield Programme	Annual Review
Do nothing	No implementation of rules	n.a.	n.a.	n.a.	n.a.	High risk for controller (fine/imprisonment) and the company (damages, prohibition of business activity of electronic data processing, neg. image, turnover, revenue, shareholder value)

Source: Data Protection Working Group | Status October 2017

6.5 Possibilities of Data Transfers



7 Links und Literature

7 Links and Literature

Court Decisions

CJEU, Decision from 24.11.2011, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v Administración del Estado, C-468/10 und C-469/10, EU:C: 2011:777.

CJEU, Decision from 1.10.2015, Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság, C-230/14, EU:C:2015:639.

CJEU, Decision from 6.10.2015, Schrems v DPC Irland, C-362/24, EU:C:2015:650.

Irish High Court, Data Protection Commissioner v. Facebook Ireland Limited & Maximilian Schrems, Az. 2016/4809P.

La Quadrature du Net and others v Commission, Case T-738/16.

Legal Journals

Schmitz, Barbara/v. Dall'Armi, Jonas, Standardvertragsklauseln – heute und morgen – Eine Alternative für den Datentransfer in Drittländer?, ZD 2016, 217ff.

Drewes, Stefan/Monreal, Manfred, Grenzenlose Auftragsdatenverarbeitung, PinG 2014, 143 ff.

Greenleaf, Graham, Global Tables of Data Privacy Laws, Privacy Laws & Business International Report 2017, 14-26. Kostenloser Download unter: ↗https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2992986.

Data Protection Authorities

↗Opinions of Article 29-Working Party

↗Decisions of Düsseldorfer Kreis
(Council of German data protection authorities)
Abgestimmte Positionen der Aufsichtsbehörden in der AG 'Internationaler Datenverkehr' am 12./13. February 2007, p. 2, II.2.

↗International Conference of Data Protection & Privacy Commissioners

Further helpful links

↗DLA Piper: Data Protection Laws of the Worlds.

The Federal Association for Information Technology, Telecommunications and New Media (Bitkom) represents more than 2,500 companies in the digital sector, including 1,700 direct members. With more than 2,000,000 employees, our members generate a domestic turnover of 190 billion Euros a year, exporting high-tech goods and services worth another 50 billion Euros. Comprising 1,000 small and medium-sized businesses as well as 400 start-ups and nearly all global players, Bitkom's members offer a wide range of software technologies, IT-services, and telecommunications or internet services. They produce hardware and consumer electronics or operate in the sectors of digital media and the network industry. 80 percent of the companies' headquarters are located in Germany with an additional amount of 8 percent in other countries of the EU and 8 percent in the USA as well as 4 percent from other regions. Bitkom supports an innovative economic policy by focusing on the modernization of the education sector and a future-oriented network policy.

Federal Association for Information Technology, Telecommunications and New Media

Albrechtstraße 10
10117 Berlin
T +49 30 27576-0
F +49 30 27576-400
bitkom@bitkom.org
www.bitkom.org

bitkom