CEJ
COMPLIANCE
ELLIANCE
JOURNAL

BETWEEN A ROCK AND A HARD PLACE – LEGAL PITFALLS OF VOLUNTARY COOPERATION OF GERMAN COMPANIES WITH GERMAN AND FOREIGN REGULATORY AND LAW ENFORCEMENT AUTHORITIES

Thomas Kopp & Valentin Pfisterer

AUTHOR

Thomas Kopp is a partner at Cleary Gottlieb Steen & Hamilton LLP, based in the firm's Frankfurt office. Thomas Kopp's practice focuses on financial institutions, corporate and sovereign clients and covers a broad range of practice areas, including corporate governance, regulatory compliance & enforcement, capital markets, mergers & acquisitions and dispute resolution, in a post-transactional context or otherwise.

Valentin Pfisterer is an associate at Cleary Gottlieb Steen & Hamilton LLP, based in the firm's Frankfurt office. Valentin regularly publishes, inter alia, on financial institutions regulatory topics and aspects of privacy and data protection in both German and European law.

ABSTRACT

German companies or German-based subsidiaries of international businesses may become subject of, or otherwise involved in, investigations by German or foreign regulatory or law enforcement authorities. In the context of such investigations, it is not unusual for the concerned company to face informal requests from German or foreign regulatory and law enforcement authorities for voluntary cooperation. Oftentimes, such requests focus on the transfer of electronic data for investigatory purposes, and such data typically relate, in whole or in part, to individuals (e.g. employees, suppliers and customers).

In these and other cases, compliance of German companies or German-based subsidiaries with informal requests from regulatory and law enforcement authorities may itself entail a compliance risk or even constitute a breach by the corporate entity of the German data protection laws resulting in criminal prosecution, administrative sanctions, or damage claims and other actions by third party individuals. This article outlines the scope of application of the German Federal Data Protection Act, introduces the applicable statutory provisions, and discusses the relevant considerations in the context of an informal request by a regulatory or law enforcement authority for voluntary cooperation in the context of global investigations, in particular where a German-based entity faces requests from authorities abroad.

TABLE OF CONTENTS

Many German companies maintain business operations or perform business activities abroad and, equally, many international businesses maintain subsidiaries in Germany. In doing so, the German companies are required to comply with the laws applicable to them in the countries where they maintain operations or perform business activities, and the German-based subsidiaries of international businesses are required to comply with German law. Against this background, in suspected cases of non-compliance with applicable laws, it is not unusual for corporate entities based in Germany to become subject of, or otherwise involved in, investigations by German or foreign regulatory or law enforcement authorities. The *Siemens* case, the *Daimler* case, the LIBOR case or, most recently, the investigations in the automotive sector are prominent examples of global investigations involving German companies or German-based subsidiaries of international businesses. In the context of such investigations, it is not unusual for the concerned company to face informal requests from German or foreign regulatory and law enforcement authorities for voluntary cooperation. Oftentimes, such requests focus on the transfer of electronic data for investigatory purposes, and such data typically relate, in whole or in part, to individuals (e.g. employees, suppliers and customers).[1] In the context of an investigation by the U.S. Department of Justice ("DOJ") or the Securities and Exchange Commission ("SEC"), for example, pursuant to a memorandum issued by the Deputy Attorney General of the DOJ on September 9, 2015 on the individual accountability for corporate wrongdoing ("Yates Memorandum"), "*to be eligible for any cooperation credit, corporations must provide to the Department all relevant facts about the individuals involved in corporate misconduct.*"[2] Given the variety of potential adverse consequences of non-cooperation including fines, sanctions, loss of cooperation credit, and negative media coverage[3], companies will typically be inclined to comply with any such informal request for voluntary cooperation including the required data transfers.

While this position is understandable, German companies and subsidiaries of international businesses located in Germany should thoroughly reflect on the legal implications of the actions required to comply with such a request.[4] The reason for this is that, under German law, informal requests by German or foreign regulatory and law enforcement authorities do not per se form a legal basis for the required actions. Rather, the German-based corporate entity has to asses, taking into account the legal rules and regulations

---

1 Tim Wybitul, *How to Conduct E-mail Reviews in Germany*, COMPLIANCE ELLIANCE JOURNAL, 59, 62 (2016).

2 DOJ, Office of the Deputy Attorney General, *Yates* Memorandum, September 9, 2015 (www.justice.gov/dag/file/769036/download), p. 3.

3 For an account of a case of operational and reputational damage as a consequence of the lack of cooperation, *see* Folker Bittmann, *Internal Investigations under German Law*, COMPLIANCE ELLIANCE JOURNAL, 74, 84 (2015).

4 On the conflicting priorities in such situations, *see* Sascha Süße & Carolin Püschel, *Collecting Evidence in Internal Investigations in the Light of Parallel Criminal Proceedings*, COMPLIANCE ELLIANCE JOURNAL, 26, 52 *et seq.* (2016).

applicable to it, whether or not it is actually permitted to meet an informal request of a German or foreign regulatory and law enforcement authority. In certain cases, compliance of the corporate entity with such an informal request may itself entail a compliance risk or even constitute a breach by the corporate entity of the laws applicable to it resulting in criminal prosecution, administrative sanctions, or damage claims and other actions by third party individuals.[5] In this context and in relation to requested transfers of personal data, the data protection laws applicable in Germany, particularly the German Federal Data Protection Act (*Bundesdatenschutzgesetz* – "FDPA"), are especially important to be taken into consideration.[6]

This article outlines the scope of application of the FDPA (I.), introduces the applicable statutory provisions, and discusses the relevant considerations in connection with an informal request by a regulatory or law enforcement authority for voluntary cooperation in the context of global investigations (II. and III.), in particular where a German based entity faces requests from authorities abroad (III.). While this article focuses on the current legal framework in Germany governed by the FDPA and the European Data Protection Directive of 1995 ("DPD"), it also takes into account the General Data Protection Regulation ("GDPR")[7] as published in the Official Journal of the European Union on May 4, 2016 by way of reference where appropriate. As from May 2018, the legal framework for the protection of personal data in the European Union will be primarily governed by the provisions of the GDPR.

I. THE SCOPE OF APPLICATION OF THE GERMAN FEDERAL DATA PROTECTION ACT

At present, the FDPA constitutes the central legal framework in the area of data pro-

---

5 *See* Sascha Süße & Carolin Püschel, *Collecting Evidence in Internal Investigations in the Light of Parallel Criminal Proceedings*, COMPLIANCE ELLIANCE JOURNAL, 26, 36 (2016): *"The collecting of evidence itself must certainly be compliant with all applicable laws, i.e. must not violate any criminal, data protection or labor laws."*

6 *See* Christian Pelz, *Ambiguities in International Internal Investigations*, COMPLIANCE ELLIANCE JOURNAL, 14, 16 (2016): "*Privacy and data protection issues are of major concern in any kind of compliance review, compliance audit and in particular in international internal investigations.*"

Under certain circumstances, stricter legal standards may apply in addition to, or in lieu of, the FDPA, such as the German Telemedia Act and the German Telecommunications Act, or in the case of the personal data of the customers of credit institutions, the principles of banking secrecy. These standards will not be addressed in this article. As to the standards applicable under German law to email reviews, *see* Tim Wybitul, *How to Conduct E-mail Reviews in Germany*, COMPLIANCE ELLIANCE JOURNAL, 59 *et seq.* (2016); Tim Wybitul & Wolf-Tassilo Böhm, *E-Mail-Kontrollen für Compliance-Zwecke und bei internen Ermittlungen*, CORPORATE COMPLIANCE-ZEITSCHRIFT, 133, 133 (2015).

7 *See* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), O.J. 2016, L 119/1 (hereinafter "GDPR").

tection in Germany. The FDPA implements the DPD which aims to harmonize the data protection regimes in all EU Member States.[8] The purpose of the DPD is *"to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data"*.[9] Correspondingly, it is the purpose of the FDPA *"to protect the individual against his/her right to privacy being impaired through the handling of his/her personal data"*.[10]

A. The Concept of "Personal Data"

The concept of "*personal data*", under German and European law, is broad[11] and encompasses any information relating to an identified or identifiable natural person, the so-called data subject.[12] Pursuant to the Article 29 Working Party, a committee of representatives of the national data protection authorities of the EU Member States, *"a person can be considered as "identified" when, within a group of persons, he or she is "distinguished" from all other members of the group."*[13] In contrast, an *"identifiable"* person is *"a person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"*.[14] Personal data within this meaning can be included, for instance, in notebook entries, personal files, minutes, documentation relating to goods, services and financial transactions, information about customers, suppliers and business partners. Such data is often significant for regulatory or criminal investigations as it can provide evidence for the behavior of one or more individuals, corporate bodies such as boards or committees or even the business practice throughout a company or an entire corporate group.

---

8 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, O. J. 1995, L 281/31 ("Data Protection Directive" or "DPD"). For information on the DPD, *see* Paul M. Schwartz &Daniel J. Solove, *Reconciling Personal Information in the United States and European Union,* CALIFORNIA LAW JOURNAL, 877, 882-884 (2014); Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures,* HARVARD LAW REVIEW, 1966, 1971-1979 (2013); Paul M. Schwartz, *Information Privacy in the Cloud,* UNIVERSITY OF PENNSYLVANIA LAW REVIEW, 1624, 1639-1642 (2013); Virginia Boyd, *Financial Privacy in the United States and the European Union: A Path to Transatlantic Supervisory Harmonization*, BERKELEY JOURNAL OF INTERNATIONAL LAW, 939, 958-967 (2006).

9 Article 1(1) DPD.

10 Section 1(1) FDPA.

11 *See* Article 29 Working Party, Opinion 4/2007 on the concept of personal data, WP 136, June 20, 2007, p. 4 (*"The Directive contains a broad notion of personal data"*). As to the common features and differences of the concepts used in the U.S. and Europe, *see* Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union,* CALIFORNIA LAW JOURNAL, 877, 881 *et seq.* (2014); Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures,* HARVARD LAW REVIEW, 1966, 1968-1992 (2013); more profoundly, James Q. Whitman, *The Two Western Cultures of Privacy: Dignity versus Liberty*, YALE LAW JOURNAL, 1151, 1153 *et seq.* (2004).

12 Section 3(1) FDPA, Article 2a) DPD.

13 Article 29 Working Party, Opinion 4/2007 on the concept of personal data, WP 136, June 20, 2007, p. 12.

14 Article 2a) DPD. For a more detailed analysis, *see* Article 29 Working Party, Opinion 4/2007 on the concept of personal data, WP 136, June 20, 2007, p. 12 *et seq*.

B. "Collection, Processing and Use" of Personal Data

The FDPA governs the "*collection, processing and use of personal data*" in Germany.[15] "*Collection*", per its definition, is the obtaining of data regarding the data subject.[16] *"Processing"*, on the other hand, includes various activities within the scope of activity of a company subject to an information request by an authority. Thus, "*processing"* captures, *inter alia*, the transfer of such personal data.[17] "*Transfer*", in turn, means the disclosure to a third party of personal data stored or obtained by means of data processing through transmission of the data to the third party or, in the terms of the DPD, the *"disclosure by transmission, dissemination or otherwise making available"* of personal data.[18]

In view of the above, the provision by companies of information relating to individuals such as employees, suppliers and customers to public authorities may be relevant under the FDPA in two respects: First, the provision by the company may qualify as transfer and, thus, processing of personal data within the meaning of the FDPA. Second, the receipt of the information by the public authority may qualify as collection of personal data within the meaning of the FDPA.

II. DATA TRANSFERS TO GERMAN REGULATORY OR LAW ENFORCEMENT AUTHORITIES

In regard to the collection of personal data by a public authority from a private sector entity, the FDPA establishes a clear distinction: In such cases, the public authority shall either inform the private sector entity of the legal provision requiring the disclosure, *i.e.* the transfer, of the relevant personal data or, alternatively, of the fact that such disclosure is voluntary.[19] In the former case, and assuming the requirements of the relevant provision are met, the private sector entity is legally obliged to transfer the relevant personal data to the public authority. In the latter case, *i.e.* in the absence of a *statutory obligation* to transfer the relevant personal data, the private sector entity, before transferring the relevant personal data, has to ensure that it is actually allowed to do so.[20]

---

15 Section 1(2) FDPA, Article 3(1) DPD. Also *see* Article 4(2) GDPR.

16 Section 3(3) FDPA. Examples in legal literature for the "collection" of personal data include the request of personal records or the active receiving of media or documentation including personal information, *see* Ulrich Dammann, *in* BDSG, Section 3 m.n. 109, (Spiros Simitis, 8th ed. 2014); *see* also Benedikt Buchner, *in* BDSG, Section 3 m.n. 26 (Jürgen Taeger & Detlev Gabel, 2nd ed. 2013).

17 Section 3(4) Sent. 1 FDPA. *See* Article 29 Working Party, Working Document on surveillance of electronic communications for intelligence and national security purposes, December 5, 2014, p. 37-38.

18 Section 3(4) Sent. 2 No. 3a) FDPA and Article 2b) DPD. Also *see* Article 4(2) GDPR.

19 Section 13(1a) FDPA.

20 Bettina Sokol & Philip Scholz, *in* BDSG, Section 13 m.n. 30 (Spiros Simitis, 8th ed. 2014); Peter Wedde, *in* BDSG, Section 13 m.n. 21 (Wolfgang Däubler, Thomas Klebe, Peter Wedde & Thilo Weichert, 5th ed. 2016);

Pursuant to the general rule set forth in Section 4(1) FDPA, the transfer of personal data by a private entity to a third party, including a requesting regulatory or law enforcement authority, requires either the *consent* of the data subject or a *statutory authorization*.

A. Consent

As regards the consent of the data subject, such consent shall be effective only when based on the *"data subject's free decision"* (Section 4a(1) FDPA).[21] Further, *"data subjects shall be informed of the purpose of collection, processing or use and, in so far as the circumstances of the individual case dictate or upon request, of the consequences of withholding consent. Consent shall be given in writing unless special circumstances warrant any other form"*.[22] Additionally, due to its voluntary nature, consent can be withdrawn at any time, removing the legal basis for the processing.[23] In an investigation context, for a company facing an information request by a public authority, it is oftentimes not a viable option to obtain the consent of the relevant data subjects. In some cases, where the relevant information relates to a vast number of individuals, this would require an excessive administrative effort; in other cases, the request for consent would make the relevant individual aware of the investigation and, thus, potentially defeat its objective and purpose. Also, with regard to employees' personal data (*see* II.B. below), there is a controversy as to whether and to what extent an employee's consent *vis-à-vis* the employer can be regarded as a free decision within the meaning of Section 4a(1) FDPA due to the imbalance of power inherent in the employment relationship, and, consequently, calls the processing of the data by the employer into question.[24] Finally, the concerned individuals may decide not to grant their consent or, after having initially granted the consent, to withdraw it at a later stage.

B. Statutory Authorizations – Legitimate Purpose, Necessity and Balancing of Interests

Jutta Stender-Vorwachs, *in* BeckOK BDSG, Section 13 m.n. 16 (Heinrich Amadeus Wolff & Stefan Brink *et al* 15th ed. 2015).

21 The concept of consent remains a legal basis for processing also under the GDPR (*see* Article 6(1) a) GDPR). The requirements for a consent to be valid under the GDPR are stipulated in Article 7 GDPR.

22 Section 4a(1) FDPA.

23 After the withdrawal of the consent by the data subject, the consent no longer constitutes a legal basis for the use of the relevant personal data. Correspondingly, the relevant personal data may no longer be used, unless a statutory authorization is available. Spiros Simitis, *in* BDSG, Section 4a m.n. 94, 96, 103 (Spiros Simitis, 8th ed. 2014); Kai-Uwe Plath, *in* BDSG, Section 4a m.n. 70 *et seq.* (Kai-Uwe Plath, 1st ed. 2013); Jürgen Taeger, *in* BDSG, Section 4a m.n. 81 *et seq.* (Jürgen Taeger & Detlev Gabel, 2nd ed. 2013).

24 The Article 29 Working Party has voiced its skepticism in this context, *see* Opinion 8/2001 on the processing of personal data in the employment context, 5062/01/EN/Final, WP 48, September 13, 2001, p. 23; Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, 2093/05/EN, WP 114, p. 11. The German Federal Labor Court (*Bundesarbeitsgericht*), though, has stated that even in an employment context there is no reason in principle why an employee's consent should not be considered a free decision, judgment of December 11, 2014 (8 AZR 1010/13).

As regards the statutory authorization to process personal data, the FDPA contains a number of provisions which explicitly allow for the processing, including transfer and collection, of personal data, subject to the requirements and limitations described therein. The common feature of these provisions is that each one of them sets forth a *specific purpose* for which, and only for which, the data controller is authorized to process the relevant personal data. While most of the statutory purposes are not relevant in an investigation context, the statutory authorizations relating to data processing *for criminal prosecution purposes*, *for averting threats to state or public security*, and *for the protection of the legitimate interests of the company or a third party* may generally be applicable.

1. Criminal Prosecution Purposes

The FDPA allows for processing of personal data for criminal prosecution purposes.[25] In this context, however, slightly different legal regimes are applicable to personal data relating to employees and personal data relating to other individuals.

Employee data. While, pursuant to Section 32(1) FDPA, personal data of an employee may be collected, processed or used to detect criminal offences, employees benefit from a higher level of data protection than other individuals. In the case of employees, documented factual indications are required that the data subject has committed a criminal offence in connection with his employment.[26] As a consequence, first, the suspicion of a *criminal offense* is required as opposed to an offense of an administrative nature.[27] Second, mere assumptions or speculations as to a potential criminal offense potentially committed by a given employee are not sufficient, as strong as they may be; actual *factual indications* are required.[28] Third, indications of a criminal offense potentially committed by a given employee unrelated to his *employment* are not in scope.[29] Fourth, the relevant indications, including the damage occurred, the potential suspects, and the indications which are at the heart of the suspicion, are to be *duly documented* in written

---

[25] Section 32(1) and 28(2) No. 2b) FDPA.

[26] Section 32(1) Sent. 2 FDPA.

[27] Achim Seifert, *in* BDSG, Section 32 m.n. 102 (Spiros Simitis, 8th ed. 2014); René Erfurth, *Der „neue" Arbeitnehmerdatenschutz im BDSG*, NEUE JURISTISCHE ONLINE-ZEITSCHRIFT, 2914, 2921 (2009); Tim Wybitul, *Das neue Bundesdatenschutzgesetz: Verschärfte Regeln für Compliance und interne Ermittlungen*, BETRIEBS-BERATER 1582, 1584 (2009).

[28] Oliver Zöll, *in* BDSG, Section 32 m.n. 50 (Jürgen Taeger & Detlev Gabel, 2nd ed. 2013); Achim Seifert, *in* BDSG, Section 32 m.n. 103 (Spiros Simitis, 8th ed. 2014); Uwe H. Schneider, *Investigative Maßnahmen und Informationsweitergabe im konzernfreien Unternehmen und im Konzern*, NEUE ZEITSCHRIFT FÜR GESELLSCHAFTSRECHT, 1201, 1206 (2010); Christiane Bierekoven, *Korruptionsbekämpfung vs. Datenschutz nach der BDSG-Novelle*, COMPUTER UND RECHT, 203, 206 (2010); René Erfurth, *Der „neue" Arbeitnehmerdatenschutz im BDSG*, NEUE JURISTISCHE ONLINE-ZEITSCHRIFT, 2914, 2920 (2009); Tim Wybitul, *Das neue Bundesdatenschutzgesetz: Verschärfte Regeln für Compliance und interne Ermittlungen*, BETRIEBS-BERATER, 1582, 1584 (2009).

[29] Oliver Zöll, *in* BDSG, Section 32 m.n. 51 (Jürgen Taeger & Detlev Gabel, 2nd ed. 2013); Achim Seifert, *in* BDSG, Section 32 m.n. 102 (Spiros Simitis, 8th ed. 2014).

form or electronically.[30] Finally, the *rights of participation of works councils* must be observed.[31] This relates to certain participation and consultation rights granted to works councils by applicable labor laws.[32]

Data relating to other individuals. To the extent applicable in an employment context[33], as well as more generally in a commercial context, the data transfer to regulatory or law enforcement authorities must otherwise meet the requirements stipulated in Section 28 FDPA.[34] This provision sets forth *various specific statutory authorizations* which allow for the processing and transfer of personal data under certain conditions including to *prosecute criminal offences*.[35] As is the case in the employment context, only the prosecution of criminal offenses, as opposed to administrative offenses, is in scope.[36] Other than that, the requirements under Section 28 FDPA are less stringent than in an employment context, and, for example, the documentation of the suspicion or the involvement of a works council, if any, are not mandatory (*see* above).

2. Averting Threats to State or Public Security

The FDPA further also allows for the processing of personal data in order *to avert threats to state or public security*.[37] The powers granted under this provision are relatively broad. This notwithstanding, it does not generally allow for the processing of personal data for public interest purposes; in using the term "*threats to state or public security",* the legislator has deliberately opted for a narrower term as opposed to a general public interest exemption.[38] Also, the provision requires a concrete risk of such a threat, a mere

---

30 Oliver Zöll, *in* BDSG, Section 32 m.n. 52 (Jürgen Taeger & Detlev Gabel, 2nd ed. 2013).

31 Section 32(3) FDPA.

32 *See*, for example, Section 75(2), 80, and 87(1) No. 6 of the Works Council Constitution Act (*Betriebsverfassungsgesetz*); for additional detail, *see* Tim Wybitul, *How to Conduct E-mail Reviews in Germany*, COMPLIANCE ELLIANCE JOURNAl, 59, 72 (2016).

33 There is some dispute in legal literature as to whether or to what extent Section 28 FDPA is applicable alongside Section 32 FDPA in an employment context, *see* Oliver Zöll, *in* BDSG, Section 32 m.n. 7 (Jürgen Taeger & Detlev Gabel, 2nd ed. 2013); Achim Seifert, *in* BDSG, Section 32 m.n. 17 (Spiros Simitis, 8th ed. 2014); Uwe H. Schneider, *Investigative Maßnahmen und Informationsweitergabe im konzernfreien Unternehmen und im Konzern*, NEUE ZEITSCHRIFT FÜR GESELLSCHAFTSRECHT, 1201, 1205 (2010); Christiane Bierekoven, *Korruptionsbekämpfung vs. Datenschutz nach der BDSG-Novelle*, COMPUTER UND RECHT, 203, 206 (2010); René Erfurth, *Der „neue" Arbeitnehmerdatenschutz im BDSG*, NEUE JURISTISCHE ONLINE-ZEITSCHRIFT, 2914, 2922 (2009).

34 *See* Jürgen Taeger, *in* BDSG, Section 28 m.n. 31 (Jürgen Taeger & Detlev Gabel, 2nd ed. 2013); similar Spiros Simitis, *in* BDSG, Section 28 m.n. 22 (Spiros Simitis, 8th ed. 2014).

35 Section 28(2) No. 2 b) FDPA.

36 Spiros Simitis, *in* BDSG, Section 28 m.n. 190 (Spiros Simitis, 8th ed. 2014); Kai-Uwe Plath, *in* BDSG, Section 28 m.n. 97 (Kai-Uwe Plath, 1st ed. 2013); Jürgen Taeger, *in* BDSG, Section 28 m.n. 146 (Jürgen Taeger & Detlev Gabel, 2nd ed. 2013).

37 Section 28(2) No. 2b) FDPA.

38 Spiros Simitis, *in* BDSG, Section 28 m.n. 190 (Spiros Simitis, 8th ed. 2014).

abstract risk is not sufficient.[39] Finally, specific statutory authorizations set forth in the laws applicable to the relevant regulatory or enforcement authorities take precedence over this particular exemption to the effect that such authorities have to rely on such specific authorizations, if any, to request the relevant data from private companies and may not rely on Section 28(2) No. 2b) FDPA where such statutory authorization does not exist or its requirements are not met.[40]

3. Protection of the Legitimate Interests of the Company or a Third Party

Finally, the FDPA allows for the processing of personal data to *protect the legitimate interests of the company or a third party*.[41] Both authorizations are to be interpreted narrowly.[42]

Legitimate interests of the company. Legitimate interests of the company within this meaning may be both monetary as well as non-monetary interests.[43] The keen interest of a requesting third party, including regulatory or law enforcement authorities, does not qualify as a legitimate interest of the company.[44] A cooperative relationship of the company with the relevant regulatory or law enforcement authority in general and the compliance with an informal request of such an authority, including to avoid potential adverse consequences of non-cooperation, should typically count among the legitimate interests of a company, the warranted narrow interpretation notwithstanding.

Legitimate interests of a third party. There is no reason in principle why regulatory or law enforcement authorities should be excluded from the term "third party". Therefore, the company facing an informal information request has to assess whether or not such information request is based on reasonable needs for information on the part of the requesting authority and whether or not such informational needs qualify as legitimate interests within this meaning.

4. Additional Requirements: Necessity and Balancing of Interests

Necessity. In each of the cases described above, the processing of the personal data must be "*necessary*" to pursue the legitimate purpose, *i.e.* to investigate the alleged criminal offence, to avert the threats to state or public security, or to protect the legitimate inter-

---

39 Kai-Uwe Plath, *in* BDSG, Section 28 m.n. 97 (Kai-Uwe Plath, 1st ed. 2013); Jürgen Taeger, *in* BDSG, Section 28 m.n.144 (Jürgen Taeger & Detlev Gabel, 2nd ed. 2013).

40 Jürgen Taeger, *in* BDSG, Section 28 m.n.146 (Jürgen Taeger & Detlev Gabel, 2nd ed. 2013); Spiros Simitis, *in* BDSG, Section 28 m.n. 192 (Spiros Simitis, 8th ed. 2014).

41 Section 28(2) No. 1 and No. 2a) FDPA.

42 Spiros Simitis, *in* BDSG, Section 28 m.n. 98 and 174 (Spiros Simitis, 8th ed. 2014).

43 Spiros Simitis, *in* BDSG, Section 28 m.n. 104 (Spiros Simitis, 8th ed. 2014); Jürgen Taeger, *in* BDSG, Section 28 m.n.55 (Jürgen Taeger & Detlev Gabel, 2nd ed. 2013).

44 Spiros Simitis, *in* BDSG, Section 28 m.n. 107 (Spiros Simitis, 8th ed. 2014).

ests of the company or a third party.[45] The term *"necessary"* is generally interpreted narrowly and strictly.[46] As a consequence, it has to be examined carefully whether the envisaged data transfer could be replaced by a less intrusive action or the corresponding goal otherwise pursued by less intrusive means.[47]

Balancing of interests. Further, in each of the cases described above, the data subject's *"legitimate interest"* in keeping his personal data undisclosed are to be adequately taken into account.[48] More precisely, in the case of data processing for the purpose of criminal prosecution, averting threats to state or public security and the protection of legitimate interests of a third party, there must not be any *"reason to believe that the data subject has such legitimate interest*" at all.[49] In other words, a data transfer may not be based on the corresponding statutory authorizations if there is at least one single reason for the concerned individual providing for a legitimate interest of such individual to maintain his personal data undisclosed. Slightly less strict, in the case of data processing for the purpose of the protection of legitimate interests of the company, the data subject must not have an "*overriding legitimate interest"* in maintaining the confidentiality of his data.[50] This requires a comprehensive proportionality assessment to evaluate the suitability of the data processing for the purpose pursued, its necessity relative to potentially less intrusive means (*see* above), as well as its adequacy, especially in regards to the type and extent of data processing.[51] In the course of this assessment, a comprehensive balancing of interests is required whereby the interests in favor of the data transfer (the self-interests of the company) are to be weighed against the interest of the data subject in keeping his data confidential. As a result of such assessment, the interests of the data

---

45 Section 28(2) No. 1 and No. 2a) and b) FDPA. *See* Article 6(1) d), e) and f) GDPR.

46 Achim Seifert, *in* BDSG, Section 32 m.n. 11 (Spiros Simitis, 8th ed. 2014); Katrin Stamer & Michael Kuhnke, *in* BDSG, Section 32 m.n. 16 (Kai-Uwe Plath, 1st ed. 2013); Oliver Zöll, *in* BDSG, Section 32 m.n. 16 (Jürgen Taeger & Detlev Gabel, 2nd ed. 2013); Spiros Simitis, *in* BDSG, Section 28 m.n. 182 *et seq.* (Spiros Simitis, 8th ed. 2014); Jürgen Taeger, *in* BDSG, Section 28 m.n. 135 *et seq.* (Jürgen Taeger & Detlev Gabel, 2nd ed. 2013).

47 Achim Seifert, *in* BDSG, Section 32 m.n. 105 (Spiros Simitis, 8th ed. 2014); Tim Wybitul, *Das neue Bundesdatenschutzgesetz: Verschärfte Regeln für Compliance und interne Ermittlungen*, BETRIEBS-BERATER, 1582, 1583 (2009).

48 Section 32(1) Sent. 2 and Section 28(2) No. 1 and No. 2 FDPA.

49 Section 28(2) No. 1 and 2 FDPA. A similar requirement is explicitly mentioned only in Article 6(1) f) GDPR (data processing necessary for the purposes of the legitimate interests pursued by a controller or a third party). However, Article 6(3) GDPR states that the legal basis of the data processing referred to in Article 6(1) c) and e) GDPR (processing necessary for compliance with a legal obligation to which the controller is subject or necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller) must be rooted in European Union law or the law of the Member State to which the controller is subject. The law of the Member State must meet a public interest objective or must be necessary to protect the rights and freedoms of others, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued. In the context of the corresponding assessment, the legitimate interests of the data subject should obviously be taken into consideration.

50 Section 28(1) Sent. 1 No. 2 FDPA.

51 Oliver Zöll, *in* BDSG, Section 32 m.n. 53 (Jürgen Taeger & Detlev Gabel, 2nd ed. 2013); Achim Seifert, *in* BDSG, Section 32 m.n. 106 (Spiros Simitis, 8th ed. 2014); Jan Pohle, *Unterlagen-, Daten- und E-Mailauswertung unter Berücksichtigung datenschutzrechtlicher Aspekte, in*: Deutsch-Amerikanische Korruptionsverfahren 309, 316 (Jürgen Wessing & Matthias Dann eds., 2013).

subject take precedence particularly in situations where the type and extent of the data processing are disproportionate to the purpose pursued.[52] Also, in the context of regulatory or criminal investigations, it is of particular relevance whether the concerned individual is a suspect, a potential witness or a person not involved in the investigated misconduct. While the FDPA also generally protects the personal data of criminal suspects[53], in connection with the proportionality assessment, the interest of not getting involved in, or subject of, a regulatory or criminal investigation may weigh stronger in the case of potential witnesses or persons unrelated to the investigated misconduct than in the case of suspects.

III. DATA TRANSFERS TO FOREIGN REGULATORY OR LAW ENFORCEMENT AUTHORITIES

The FDPA applies where the controller is either located or collects or processes personal data in Germany.[54] A German-based corporate entity subject to an informal information request by a foreign regulatory or law enforcement authority has to assess, in addition to the legality of the preparatory data collection, the permissibility of the envisaged data transfer in light of Sections 4b and 4c FDPA.[55] These provisions establish specific requirements for the transfer of personal data across borders which apply in addition to the requirements applicable in a domestic context (*see* II. above).[56] They further differentiate between data transfers to recipients located in EU or EEA Member States (*see* A. below) and data transfers to recipients located in what is known as Third Countries (*see* B. below).

A. Regulatory or Law Enforcement Authorities located in EU or EEA Member States

Data transfers to recipients located in EU or EEA Member States are primarily governed by Section 4b(1) FDPA which reads: *"The transfer of personal data to bodies 1. in other Member States of the European Union, 2. in other states parties to the Agreement on the European Economic Area or 3. institutions and bodies of the European Communities shall be subject to (...) Sections 28 to 30a in accordance with the laws and agreements ap-*

---

52 Spiros Simitis, *in* BDSG, Section 28 m.n. 180 (Spiros Simitis, 8th ed. 2014); Kai-Uwe Plath, *in* BDSG, Section 28 m.n. 53 and 95 *et seq.* (Kai-Uwe Plath, 1st ed. 2013); Jürgen Taeger, *in* BDSG, Section 28 m.n. 61 *et seq.* (Jürgen Taeger & Detlev Gabel, 2nd ed. 2013).

53 *See* Spiros Simitis, *in* BDSG, Section 28 m.n. 190 et. seq and 195 (Spiros Simitis, 8th ed. 2014); Kai-Uwe Plath, *in* BDSG, Section 28 m.n. 97 (Kai-Uwe Plath, 1st ed. 2013); Jürgen Taeger, *in* BDSG, Section 28 m.n. 141 and 145 (Jürgen Taeger & Detlev Gabel, 2nd ed. 2013). Also *see* Article 10 GDPR.

54 Section 1(5) FDPA.

55 Detlev Gabel, *in* BDSG, Section 4b m.n. 9 (Jürgen Taeger & Detlev Gabel, 2nd ed. 2013) Spiros Simitis, *in* BDSG, Section 4b m.n. 38-39 (Spiros Simitis, 8th ed. 2014); Philipp Räther & Nicolai Seitz, *Übermittlung personenbezogener Daten in Drittstaaten Angemessenheitsklausel, Safe Harbor und die Einwilligung,* MULTIMEDIA UND RECHT, 425, 426 (2002).

56 Section 28 *et seq.* FDPA.

plicable to such transfer, in so far as transfer is effected in connection with activities which fall in part or in their entirety within the scope of the law of the European Communities." Hence, the transfer of personal data to recipients in EU or EEA Member States is generally subject to the requirements applicable in a domestic context as discussed above, although in accordance with the laws and agreements applicable to such transfer, inasmuch as the transfer is effected in connection with activities which fall either entirely or in part within the scope of the law of the European Communities.[57]

1. Prerequisite Requirements: Precedence Rule and Limited Scope of Applicability

This requirement raises at least two potential pitfalls to companies willing to comply with an informal request from an EU or EEA authority.

Precedence rule. First, the provision states that the cross-border transfer of personal data has to occur "*in accordance with the laws and agreements applicable to such transfer"*.[58] This requirement implies that the envisaged data transfer, including its limits and conditions, is subject to special laws or bilateral or multilateral agreements, if any such law or agreement applies in the specific case.[59] Such laws or agreements may take precedence over the general data protection provisions contained in the FDPA and set forth the legal requirements applicable to the envisaged transfer.[60] As a consequence, special attention should be paid to whether or not a specific legal regime for cross-border data transfer exists in a given case and, if so, whether the specific requirements set forth in such regime are met.

Limited scope of applicability. Second, the provision generally only authorizes cross-border data transfers to the extent *"activities which fall in part or in their entirety within the scope of the law of the European Communities"* are affected. This refers to what was formerly known as the first pillar of the European Union pursuant to the Maastricht Treaty and, broadly speaking, comprised the area of economic and trade cooperation.[61] The first pillar should be distinguished from what was formerly known as the second pillar (Common Foreign and Security Policy) and the third pillar (Police and Judicial Cooperation in Criminal Matters).[62] The wording of Section 4b FDPA should be seen

---

57 Detlev Gabel, *in* BDSG, Section 4b m.n. 10-13 (Jürgen Taeger & Detlev Gabel, 2nd ed. 2013); Spiros Simitis, *in* BDSG, Section 4b m.n. 25-37 (Spiros Simitis, 8th ed. 2014).

58 Section 4b(1) FDPA.

59 Spiros Simitis, *in* BDSG, Section 4b m.n. 37 and 40 (Spiros Simitis, 8th ed. 2014).

60 LUTZ BERGMANN, ROLAND MÖHRLE & ARMIN HERB, BDSG, Section 4b m.n. 24 (loose-leaf booklet ed. 2014); Spiros Simitis, *in* BDSG, Section 4b m.n. 40 (Spiros Simitis, 8th ed. 2014); Detlev Gabel, *in* BDSG, Section 4b m.n. 12 (Jürgen Taeger & Detlev Gabel, 2nd ed. 2013).

61 Detlev Gabel, *in* BDSG, Section 4b m.n. 11 and 14 (Jürgen Taeger & Detlev Gabel, 2nd ed. 2013); Spiros Simitis, *in* BDSG, Section 4b m.n. 33 (Spiros Simitis, 8th ed. 2014).

62 Detlev Gabel, *in* BDSG, Section 4b m.n. 11 and 14 (Jürgen Taeger & Detlev Gabel 2nd ed. 2013).

in light of Art. 3(2) DPD. Pursuant to this provision, the DPD shall not apply to the processing of personal data *"in the course of an activity which falls outside the scope of Community law (...) and in any case to processing operations concerning public security, defense, State security (...) and the activities of the State in areas of criminal law"*.[63] Rather, the protection of personal data in connection with data transfers between EU Member States in the area of police and judicial cooperation in criminal matters is, since recently, governed by a particular directive.[64] As to the qualification of a given activity as falling inside or outside the scope of Community law, neither the wording nor case law of German courts give clear guidance as to which activity should be taken into account in this context – the business activities of the company (which should usually fall within the scope of the first pillar) or the investigative activities of the regulatory or law enforcement authorities to which the company is supposed to contribute by transferring the data (which may fall into the scope of the third pillar). In the so-called *PNR* decision of 2006, however, the European Court of Justice ("ECJ") implicitly decided in favor of the latter.[65] In the corresponding case, the ECJ had been asked by the European Parliament to annul the so-called PNR Agreement concluded between the EU and the U.S. in 2004.[66] The 2004 PNR Agreement allowed for the competent U.S. authority to access the PNR data stored in the reservation/departure control systems of air carriers located within the territory of EU Member States for the purpose of *"preventing and combating terrorism and related crimes and other serious crimes that are transnational in nature, including organised crime"*. In the decision handed down by the ECJ, the ECJ held that the 2004 PNR Agreement was invalid due to the lack of a suitable legal basis in Community law. The ECJ explained that *"the transfer of PNR data to CBP constitutes processing operations concerning public security and the activities of the State in areas of criminal law"*[67] and, therefore, could not be based on the DPD or otherwise on Com-

---

63 The scope of application of the GDPR is similarly restricted to the processing of personal data *"in the course of an activity which falls within the scope of Union law"* (which is, admittedly, more extensive than the law of the (former) European Communities) (*see* Article 2(2) a) GDPR). However, the GDPR also excludes from its scope of application data processing *"by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties"* (Article 2(2) d) GDPR) which mirrors what is set forth in Article 3(2) DPD.

64 Directive of the European Parliament and of the Council of 04/27/2016 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, and repeating Council Framework Decision 2008/977/JHA, O.J. 2016, L 119/89.

65 *See* ECJ, judgment May 30, 2006 (*PNR*) – C-317/04 – m.n. 56. The acronym PNR stands for Passenger Name Record data (specific files on every passenger and journey created by air carriers) and relates to the transatlantic transfer of information contained in these files for law enforcement purposes. For additional detail, *see* Valentin M. Pfisterer, *PNR in 2011: Recalling Ten Years of Transatlantic Cooperation in PNR Information Management,* THE UNIVERSITY OF MIAMI NATIONAL SECURITY & ARMED CONFLICT LAW REVIEW, 114, 120 *et seq.* (2012).

66 Agreement between the European Community and the United States of America on the processing and transfer of Passenger Name Record data by air carriers to the United States Department of Homeland Security, O.J. 2004, L 183/84.

67 ECJ, judgment May 30, 2006 (*PNR*) – C-317/04 – m.n. 56.

munity law.[68] Against this background, there are good arguments that at least the transfer of personal data by companies for investigative purposes of law enforcement authorities should be outside the scope of the law of the European Communities and, thus, cannot be justified under Section 4b(1) FDPA.[69] Consequently, such data transfer would be subject to the stricter requirements under Section 4b(2) FDPA. Pursuant to this provision, data transfers to recipients located in the EU or the EEA *"when effected outside of activities which fall in part or in their entirety within the scope of the law of the European Communities"* are also subject to Section 4b(1) FDPA. In addition, however, the provision states that such *"transfer shall not be effected in so far as the data subject has a legitimate interest in excluding transfer, in particular if an adequate level of data protection is not guaranteed".*[70] As this standard equally applies to data transfers to recipients located in so-called Third Countries, it shall be discussed below (*see* B. below).

2. Statutory Authorizations as Applicable in a Domestic Context

In addition to the requirements outlined above and by reference to Sections 28 *et seq.* FDPA,[71] data transfers to recipients located in EU or EEA Member States must also meet the criteria applicable in a domestic context. Hence, the purpose for which the data is transferred must correspond to one or more of the purposes explicitly specified in these provisions (including criminal prosecution, averting threats to state or public security, and the protection of the legitimate interests of the company or a third party) and the additional requirements (necessity and balancing of interests) have to be met (*see* II.B. above).

B. Regulatory or Law Enforcement Authorities located in Third Countries

Section 4b(2) FDPA provides the legal framework for cross-border data transfers to both recipients located in EU or EEA Member States, such transfer falling *"outside of activities which fall in part or in their entirety within the scope of the law of the European Communities"* (*see* III.A.1.) above), and to recipients located in non-EU and non-EEA countries (so-called Third Countries), *prima facie* irrespective of the nature of the data to be transferred. In doing so, it establishes even stricter requirements for such data transfers compared to the requirements applicable in a EU- or EEA-internal context

---

[68] ECJ, judgment May 30, 2006 (*PNR*) – C-317/04 – m.n. 57 and 60; *see also* Valentin M. Pfisterer, *PNR in 2011: Recalling Ten Years of Transatlantic Cooperation in PNR Information Management,* THE UNIVERSITY OF MIAMI NATIONAL SECURITY & ARMED CONFLICT LAW REVIEW, 114, 123 (2012).

[69] This notwithstanding, representatives of the German data protection authorities have indicated that they would look at the business activity of the company only which, as mentioned above, should usually fall within the scope of the law of the (former) European Communities and, therefore, within the scope of the DPD and Section 4b FDPA.

[70] Section 4b(2) FDPA.

[71] Section 4b(1) FDPA.

(such transfer falling within the area of the first pillar of the EU).[72] Pursuant to this provision, data transfers to recipients located in Third Countries are generally also subject to the requirements applicable in a EU- or EEA-internal context. In addition, however, Section 4b(2) FDPA states that such *"transfer shall not be effected in so far as the data subject has a legitimate interest in excluding transfer, in particular if an adequate level of data protection is not guaranteed"*.

1. Prerequisite Requirements: Precedence Rule and Limited Scope of Applicability

By reference to Section 4b(1) FDPA, data transfers to Third Countries are subject to the precedence rule and the limited scope of applicability as is the case for EU- or EEA-internal data transfers. Similar to what was discussed above, this requirement raises two potential pitfalls to companies willing to comply with an informal request from a Third Country authority (*see* A.1.) above).

Precedence rule. The transfer of personal data to recipients located in Third Countries has to be effected "*in accordance with the laws and agreements applicable to such transfer"* such laws and agreements, if applicable, taking precedence over data transfers based on the FDPA.[73] If, in a given case, such a treaty is applicable, the FDPA no longer serves as a suitable legal base for a transfer of personal data.

Limited scope of applicability. Further, by reference to the requirements applicable in a EU- or EEA-internal context, cross-border data transfers to recipients located in Third Countries are only admissible with regard to "*activities which fall in part or in their entirety within the scope of the law of the European Communities"*.[74] As a consequence, any data transfer to occur in the area of foreign and security policy or police and judicial cooperation in criminal matters, as opposed to the area of economic and trade cooperation, is out of scope and may not be based on Section 4b(2) FDPA.[75] Data transfers in these areas typically occur based on treaties on legal and administrative assistance ("MLATs").[76] Examples are the U.S.-Germany MLAT from 2003[77] or the so-called

---

[72] Detlev Gabel, *in* BDSG, Section 4b m.n. 14-17 (Jürgen Taeger & Detlev Gabel, 2nd ed. 2013); Spiros Simitis, *in* BDSG, Section 4b m.n. 38-40 (Spiros Simitis, 8th ed. 2014). The requirements and conditions for transfers of personal data to Third Countries are extensively regulated in Article 44 *et seq* GDPR.

[73] Section 4b(1) FDPA. *See* LUTZ BERGMANN, ROLAND MÖHRLE &ARMIN HERB, BDSG, Section 4b m.n. 24 (loose-leaf booklet ed. 2014); Spiros Simitis, *in* BDSG, Section 4b m.n. 40 (Spiros Simitis, 8th ed. 2014); Detlev Gabel, *in* BDSG, Section 4b m.n. 12 (Jürgen Taeger & Detlev Gabel, 2nd ed. 2013).

[74] Section 4b(2) read in connection with Section 4b(1) FDPA.

[75] Detlev Gabel, *in* BDSG, Section 4b m.n. 11 and 14 (Jürgen Taeger & Detlev Gabel, 2nd ed. 2013); Spiros Simitis, *in* BDSG, Section 4b m.n. 33 (Spiros Simitis, 8th ed. 2014).

[76] LUTZ BERGMANN, ROLAND MÖHRLE & ARMIN HERB, BDSG, Section 4b m.n. 24; Detlev Gabel, *in* BDSG, Section 4b m.n. 12 (Jürgen Taeger & Detlev Gabel, 2nd ed. 2013).

[77] *See* Treaties and other international Acts Series 09-1018, Mutual Legal Assistance Treaty between the United States of America and Germany, October 14, 2003 (www.state.gov/documents/organization/188782.pdf).

U.S.-EU Umbrella Agreement from 2015[78] which both, notably enough, allow for the exchange of personal data between law enforcement authorities as opposed to between private sector companies based in one country and a public authority of another country.[79] As to the qualification of a given activity as falling within or outside the scope of Community law, it is unclear which activity should be taken into account in this context – the business activities of the company or the investigative activities of the regulatory or law enforcement authorities to which the company is supposed to contribute by transferring the data. There are, however, good arguments that at least the transfer of personal data by companies for investigative purposes of law enforcement authorities located in Third Countries should be perceived as falling outside the scope of the law of the European Communities and, thus, cannot be justified under Section 4b(2) FDPA (*see* A.1.) above). This is consistent with a statement made by EU Commissioner of Justice, *Vera Jourova: "The Commission's view is that personal data held by private companies in the EU should not, in principle, be directly accessed by or transferred to foreign enforcement authorities outside of formal channels of cooperation, such as for example the Mutual Legal Assistance treaties (MLATs)."*[80]

2. Adequate Level of Data Protection

In addition, cross-border transfers to recipients located in Third Countries are generally inadmissible to the extent that the "*data subject has a legitimate interest"* in keeping his data confidential which is deemed to be the case if the Third Country does not afford an "*adequate level of data protection"*.[81] Such adequacy is assessed in light of all attendant circumstances. Particular consideration is given to the nature of the data, the purpose, the duration of the proposed data processing operation, the country of origin, the recipient country and the legal norms, professional rules and security measures which apply to the recipient.[82] By virtue of the DPD, the European Commission is authorized to find that a certain Third Country ensures an adequate level of protection within the meaning

---

78 Agreement between the United States of America and the European Union on the Protection of Personal Information relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offenses. Also *see* the corresponding Fact Sheet, MEMO/15/5612 (europa.eu/rapid/press-release_MEMO-15-5612_de.htm).

79 The requirements set forth in the FDPA may correspond to those established in Article 47 GDPR. Any judgment of a court or tribunal and any decision of an administrative authority of a Third Country requiring a controller or processor to transfer or disclose personal data may only be recognized or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty in force between the requesting Third Country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to Article 44 *et seq.* GDPR.

80 Parliamentary Questions, Answer given by Ms. Jourova on behalf of the European Commission, March 4, 2015 (www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2014-010602&language=EN).

81 Section 4b(2) Sent. 2 FDPA. As to the adequacy criterion, *see* Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures,* HARVARD LAW REVIEW, 1966, 1979-1992 (2013); Nikhil S. Palekar, *Privacy Protection: When is "Adequate" actually Adequate?*, DUKE JOURNAL OF COMPARATIVE & INTERNATIONAL LAW, 549 *et seq.* (2007/08).

82 Section 4b(3) FDPA. For transfers based on an adequacy decision by the Commission (and the criteria which taken into account), *see* Article 45 GDPR.

of the DPD.[83] Based thereon, the European Commission has taken a number of adequacy decisions[84] including with respect to the U.S., although not generally but rather limited to certain contexts such as the transfer of PNR data (in connection with the current PNR Agreement)[85] or of account data (in connection with the SWIFT Agreement).[86] Only recently, however, in its *Safe Harbor* decision, the ECJ struck down an adequacy decision by the European Commission in relation to the U.S. highlighting the uncontrolled mass surveillance of personal data by U.S. government agencies.[87] In its decision, the ECJ further emphazised that national data protection authorities may independently examine whether or not the level of data protection afforded in the recipient's home jurisdiction is adequate—even where the European Commission has adopted an adequacy decision in respect of the relevant country.[88] Also, in addition to the level of data protection, other aspects may qualify as a legitimate interest and consequently exclude a cross-border data transfer. It may therefore be relevant whether or not the requesting Third Country authority, under the rules and regulations applicable to it, is legally entitled to collect the relevant data, whether or not the information request is otherwise lawful or unlawful, or, again, whether or not the requesting Third Country authority has formal means at its disposal to request and obtain the relevant data.[89] In addition, it might also be relevant whether the concerned individual is a suspect, a potential witness or a person not involved in the wrongdoing being investigated (*see* II.B.4.) above).[90]

In cases where no adequate level of protection is provided for, or where the data subject has another legitimate interest in keeping his data undisclosed, Section 4b(2) FDPA cannot serve as a legal basis for a data transfer to a regulatory or law enforcement authority, subject to a number of explicitly specified exemptions discussed below (*see* 4. be-

---

83 Article 25(6) DPD.

84 *See* ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

85 *See* Article 19 of the Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, O.J. 2012, L215/5. For additional detail on the 2012 PNR Agreement, *see* Valentin M. Pfisterer, *PNR in 2011: Recalling Ten Years of Transatlantic Cooperation in PNR Information Management,* THE UNIVERSITY OF MIAMI NATIONAL SECURITY & ARMED CONFLICT LAW REVIEW, 114, 131 (2012).

86 *See* Article 6 of the (Second) Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program, O.J. 2010, L8/11. For additional detail on the (Second) SWIFT Agreement, *see* Valentin M. Pfisterer, *The Second SWIFT Agreement Between the European Union and the United States of America – An Overview*, GERMAN LAW JOURNAL, 1173, 1182-1187 (2010).

87 ECJ, Judgment of October 6, 2015 (*Schrems*) – C-362/14 – m.n. 105; as to this decision and its consequences for transatlantic data transfers, *see* Christian Galetzka & Kevin Rodler, *Goodbye Safe Harbor USA? – Datentransfer in die USA nach der Safe Harbor-Entscheidung des EuGH,* COMPLIANCE BERATER, 470 *et seq.* (2015).

88 ECJ, Judgment of October 6, 2015 (*Schrems*) – C-362/14 – m.n. 66.

89 Representatives of the German data protection authorities have indicated that they consider the existence of a mutual legal assistance treaty, and therefore an "official" channel for the requesting authority to request and obtain the relevant data, as a relevant factor in this context.

90 In particular in the case of an uninvolved person, her interest in not getting involved in the "mills" of the judicial system of a Third Country might qualify as a relevant criterion.

low).

3. Statutory Authorizations as Applicable in a Domestic Context

In addition to meeting the prerequisite requirements and the recipient affording an adequate level of data protection (and the data subject not having another legitimate interest in keeping his data undisclosed) as outlined above, by reference to Section 4b(1) FDPA (and, ultimately, to Sections 28 *et seq.* FDPA),[91] data transfers to recipients located in Third Countries must fulfill the criteria applicable in a domestic context. Hence, the purpose for which the data is transferred must correspond to one or more of the purposes explicitly specified in these provisions (including criminal prosecution, averting threats to state or public security, and the protection of the legitimate interests of the company or a third party) and the additional requirements (necessity and balancing of interests) have to be met (*see* II.B. above).

4. Specific Statutory Exemptions for Data Transfers to Third Countries not Affording an Adequate Level of Data Protection

The FDPA stipulates a number of specific exemptions from the general prohibition of the cross-border transfer of personal data to a Third Country in cases where such Third Country does not afford an adequate level of data protection (Section 4c(1) FDPA).[92] These exemptions are fairly limited in scope.[93]

Limited scope of applicability. The exemptions for data transfers to Third Countries not affording an adequate level of data protection are only available *"in connection with activities which fall in part or in their entirety within the scope of the law of the European Communities"*.[94] As discussed above, it is unclear which activity should be taken into account in this context. There are, however, good arguments that at least the transfer of personal data by companies for investigative purposes of law enforcement authorities located in Third Countries should be perceived as falling outside the scope of the law of the European Communities and, thus, cannot be justified under Section 4c(1) FDPA (see II.B. above).

As to the specific exemptions, in addition to the data subject's consent,[95] the data transfer is, *inter alia*, permissible if the transfer is necessary on "*important public interest*

---

[91] Section 4b(1) FDPA.

[92] For the requirements and limits of a data transfer in the absence of an adequacy decision, *see* Article 49 GDPR.

[93] Article 29 Working Party, Working Document on a mutual understanding of Article 26 (1) of the Directive 95/46/E, 24. Oktober 1995, WP 114, 25. November 2005, p. 9; *see* also Spiros Simitis, *in* BDSG, Section 4c m.n. 20 (Spiros Simitis, 8th ed. 2014).

[94] Section 4c(1) FDPA.

[95] For the requirements of an effective consent, *see* II.A. above.

grounds" or for the "*establishment, exercise or defense of legal claims in court"*.[96]

Important public interest grounds. The term "*important public interest grounds"* is not defined or otherwise rendered more precisely in the FDPA or the DPD. Based on the wording, the term is, on the one hand, broader than the term *"for averting threats to state or public security"* used in Section 28 FDPA as it does not necessarily require a threat of the mentioned sort. On the other hand, the term is narrower as not all public interest grounds are sufficient but only *"important"* ones. Investigations of merely administrative offences, as opposed to criminal offences, for example, may not be of sufficient importance to establish the necessary public interest. Further, pursuant to the Article 29 Working Party, a unilateral decision by the requesting authority does not *per se* qualify as relevant important public interest, and it is not to the requesting authority to decide independently whether or not its interest qualifies as an important public interest within this meaning.[97] The reasoning of the Article 29 Working Party is as follows: *"On this point the drafters of the Directive clearly did envisage that only important public interests identified as such by the national legislation applicable to data controllers established in the EU are valid in this connection. Any other interpretation would make it easy for a foreign authority to circumvent the requirement for adequate protection in the recipient country laid down in Directive 95/46. On the other hand, Recital 58 of Directive 95/46*[98] *refers, with regard to this provision, to cases in which international exchanges of data might be necessary "between tax or customs administrations in different countries" or "between services competent for social security matters". This specification, which appears to relate only to investigations of particular cases, explains the fact that this exception can only be used if the transfer is of interest to the authorities of an EU Member State themselves, and not only to one or more public authorities in the third country."*[99] Finally, and also in view of Recital 58 of the DPD, there is some dispute as to whether the important public interest-exemption is at all available to private companies and other private sector entities, given that the examples mentioned in the Recital – and the line of argument brought forward by the Article 29 Working Party – only refer to data transfers between public authorities as opposed to between private sector companies and public authorities.[100]

---

96 Section 4c(1) No. 4 FDPA (German-language version).

97 Article 29 Working Party, Working document on a common interpretation of Article 26 (1) of Directive 95/46/EC of 24 October 1995, WP 114, 25 November 2005, p. 14; Opinion 6/2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States, WP 66, 24 October 2002, p. 6. In this context, the GDPR clarifies that the important reasons of public interest must be recognized in Union law or in the law of the Member State to which the controller is subject (Article 49(4) GDPR).

98 Recital No. 58 of the DPD mentions "cases of international transfers of data between tax or customs administrations or between services competent for social security matters" as potential cases for the important public interest-exemption to apply.

99 Article 29 Working Party, Working document on a common interpretation of Article 26 (1) of Directive 95/46/EC of 24 October 1995, WP 114, 25 November 2005, p. 15.

100 *See* on the one hand: Detlev Gabel, *in* BDSG, Section 4c m.n. 10 (Jürgen Taeger & Detlev Gabel, 2nd ed. 2013); on the other hand: Wolfgang Däubler, *in* BDSG, Section 4c m.n. 8 (Wolfgang Däubler, Thomas Klebe, Peter Wedde & Thilo Weichert, 4th ed. 2014).

Establishment, exercise or defense of legal claims in court. The FDPA also allows for data transfers to Third Countries not affording an adequate level of data protection for purposes of the *"establishment, exercise or defense of legal claims in court"*.[101] While the exemption applies to and allows for data transfers in connection with all sorts of court proceedings, it is not applicable in administrative and other out-of-court proceedings. Therefore, based on its wording, the provision does not allow for data transfers in connection with investigations by regulatory and law enforcement authorities prior to, or entirely unrelated to, any such court proceedings.[102] Further, pursuant to the Article 29 Working Party, this exemption is only available *"if the rules governing criminal or civil proceedings applicable to this type of international situation have been complied with, notably as they derive from the provisions of the Hague Conventions of 18 March 1970 ("Taking of Evidence" Convention) and of 25 October 1980 ("Access to Justice" Convention)."*[103]

Additional requirements: necessity and balancing of interests. In both cases, data transfers on important public interest grounds and for the establishment, exercise or defense of legal claims in court, the data transfer must be "*necessary*" for the pursuit of the relevant objective.[104] In this respect, as discussed above, a data transfer is only permissible where the information request of the Third Country authority cannot be satisfied by less intrusive means including by formal channels of administrative or legal cooperation (*see* II.B.4. and III.A.1. and B.2. above).

Statutory authorizations as applicable in a domestic context. Finally, in addition to meeting the above-mentioned requirements, data transfers to recipients located in Third Countries not affording an adequate level of data protection must fulfill the criteria applicable in a domestic context.[105] Hence, the purpose for which the data is transferred must correspond to one or more of the purposes explicitly specified in these provisions (including criminal prosecution, averting threats to state or public security, and the protection of the legitimate interests of the company or a third party) and the additional requirements (necessity and balancing of interests) have to be met (*see* II.B. above).

---

[101] Section 4c(1) No. 4 FDPA (German-language version).

[102] Interestingly enough, the authorized English-language versions of both the DPD and the FDPA do not contain the addition "in court". This inconsistency has caused and continues to cause significant uncertainty with respect to the applicability of the relevant provision to administrative or similar out-of-court proceedings.

The addendum "in court" does not appear in Article 49 (1) e) GDPR. Under the GDPR, this exemption may consequently allow for German companies and individuals to transfer personal data for the purpose of the establishment of legal claims or legal defenses, including in administrative and other out-of-court proceedings.

[103] Article 29 Working Party, Working document on a common interpretation of Article 26 (1) of Directive 95/46/EC of 24 October 1995, WP 114, 25 November 2005, p. 15.

[104] Section 4c(1) No. 4 FDPA.

[105] Detlev Gabel, *in* BDSG, Section 4c m.n. 4 (Jürgen Taeger & Detlev Gabel, 2nd ed. 2013); Spiros Simitis, *in* BDSG, Section 4c m.n. 6 (Spiros Simitis, 8th ed. 2014).

5. Specific Permit by Competent Data Protection Authority

Lastly, the FDPA allows for the cross-border transfer of personal data to Third Countries, irrespective of whether or not affording an adequate level of data protection, based on a specific permit by the competent German data protection authority.[106] Accordingly, the competent German data protection authority may authorize individual transfers or certain categories of transfers of personal data to bodies located in Third Countries if the controller guarantees adequate safeguards with respect to the protection of privacy and the exercise of the corresponding rights.[107] This approach obviously requires that the company asks for and is granted adequate safeguards from the requesting Third Country authority, informs the competent German data protection authority of the envisaged data transfer in order to obtain the necessary permit, and is granted the requested permit. This option may oftentimes not be available for the corporate entity concerned, given that a public authority is generally unlikely to contractually assure a certain treatment of the relevant data, in particular in an investigation context.

IV. SUMMARY AND OUTLOOK

Corporate entities based in Germany which face an informal request from a German or foreign regulatory or law enforcement authority for the transfer of personal data will typically be inclined to comply with such an informal request, given the variety of potential adverse consequences of non-cooperation including fines, sanctions, loss of cooperation credit, and negative media coverage. In certain cases, however, compliance of the corporate entity with such an informal request may itself entail a compliance risk, constitute a breach by the corporate entity of the laws applicable to it, and result in criminal prosecution, administrative sanctions, or damage claims and other actions by third party individuals. In this context and in relation to requested transfers of personal data, the data protection laws applicable in Germany, particularly the FDPA, are especially important to be taken into consideration.

The FDPA establishes a complex and strict regime for the transfer of personal data to recipients, including regulatory and law enforcement authorities, both in Germany and abroad. The requirements for data transfers to German regulatory and law enforcement authorities are already rather strict. This is even more true for data transfers to regulatory and law enforcement authorities located in EU or EEA Member States or even in

---

[106] Section 4c(2) FDPA.

[107] Section 4c(2) FDPA. For additional detail, *see* Philipp C. Räther & Nicolai Seitz, *Übermittlung personenbezogener Daten in Drittstaaten – Angemessenheitsklausel, Safe Harbor und die Einwilligung,* MULTIMEDIA UND RECHT, 425 *et seq.* (2002) and Philipp C. Räther & Nicolai Seitz, *Ausnahmen bei Datentransfer in Drittstaaten - Die beiden Ausnahmen nach § 4c Abs. 2 BDSG: Vertragslösung und Code of Conduct*, MULTIMEDIA UND RECHT, 520 *et seq.* (2002).

Third Countries. Particularly strict requirements apply to data transfers to recipients, including regulatory and law enforcement authorities, located in Third Countries which do not afford an adequate level of data protection, especially where the data are transferred for criminal prosecution and similar not strictly business-related purposes.

In the past, companies facing an informal request for the transfer of personal data by a public authority may have considered compliance with German data protection laws a minor priority, especially when approached by authorities from Third Countries. In view of what is stated in the *Yates* Memorandum[108], this may be particularly true in the context of DOJ or SEC investigations. Also, sanctions in Germany, if any, were usually considered soft in comparison to the fear of much more severe sanctions in Third Countries including the U.S. As of the entry into force of the GDPR in May 2018, however, this is likely to change. Based on the GDPR, once applicable, the competent national data protection authorities will be authorized to impose fines in the event of a violation of the GDPR in the amount of up to EUR 20 Million or 4% of the average worldwide annual sales of a company.[109]

[108] DOJ, Office of the Deputy Attorney general, *Yates* Memorandum, September 9, 2015 (www.justice.gov/dag/file/769036/download), p. 3.

[109] Article 83(6) GDPR.