

Transfer of data out of the European Union
Application of EU and German Data Protection Law

by Dr. Axel Freiherr von dem Bussche, LL.M.

A. Legal Background

General principles of European Data Protection Law

In particular fundamentals of Directive 95/46/EC

B. Application of German Data protection law

1. The German Data Protection System

General Principles

- Collection, processing and use of personal data is prohibited unless the data subject has expressed its consent or it is legally permitted
- Legal permission
- Consent

Additional requirements if data are transferred to the US

- No transfer without adequate standard of data protection
- Exceptions – Consent or performance of contract
- Exceptions – Adequate safeguards
Contractual clauses, Safe Harbour Principles, Binding Corporate Rules

2. When does German data protection law apply?

- Collection, processing and use of personal data on German territory by US-registered companies
- US-parent company has subsidiaries in the Germany
- Commissioned collection, processing or use of personal data

C. Special Matters

- Whistle-Blowing
- Cloud Computing
- E-Discovery
- US-Websites for EU market

A. Legal Background

General principles of European Data Protection Law

Data protection has always been handled differently in the European legal area and the United States.

Developments of a frontier free European Market and of the so called 'information society' increase the cross-frontier flows of personal data between Member States of the EU and third countries as the US. In order to remove potential obstacles to such flows and to ensure a high level of protection within the EU, data protection legislation has been harmonised.

- The fundament of European data protection law is the directive 95/46/EC 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. It sets forth the most important underlying principles of European data protection law:
 - an individual has a right to know what data is being processed about them;
 - personal data has to be processed fairly and lawfully;
 - personal data must be kept for no longer than is necessary and must be accurate and up-to-date;
 - personal data must be, at all times, kept secure and where processed by a third party be managed securely; and
 - personal data should not be transferred outside the European Economic Area to any other country that does not have adequate protection for the rights of the individual.

European data protection law is not tailored according to the problems of specific areas (e.g. M&A transactions) but applies whenever personal data is collected,, proc-

essed in any way or used. The individual's right of privacy is strictly adhered to and influences all acts of European legislation in the field of data protection.

The United States on the other hand chose a rather sector-specific approach. Legislation, regulation and self-regulation are used to handle personal data in specific areas. The non-public sector in general is not too systematically regulated with regard to data protection. Therefore, cross-boarder data flow between European countries and the US faces numerous problems, the most crucial of which is that the US is regarded to have a data protection regime that is not meeting the European standard so that data transfer to the US requires special precautions.

Against this background, the European Commission engages in dialogues with non-EU countries in order to ensure a high level of protection when exporting personal data to those countries. It also initiates studies on the development on European and international level on the state of data protection.

The protection of personal data has also been incorporated in Article 8 of Charter of fundamental rights of the European Union. This Charter is, however, not legally binding.

B. Application of German Data Protection Law

1. *The German Data Protection System*

General principles:

- Collection, processing and use of personal data is prohibited, unless the data subject has expressed its consent or it is legally permitted

§ 4 sec. 1 German Federal Data Protection Act (BDSG)

The collection, processing and use of personal data shall be admissible only if permitted or prescribed by this Act or any other legal provision or if the data subject has consented.

“Personal Data” means any information concerning the personal or material circumstances of an identified or identifiable individual (the data subject)

“Collection” means the acquisition of data on the data subject;

“Processing” means the storage, modification, transfer, blocking and erasure of personal data

“Use” means any utilisation of personal data other than processing

- Legal permission

The most important provision with regard to legal permissibility of collection, processing or use of personal data is § 28 BDSG. In any case, under German data protection law, in connection with the collection of personal data, the purposes for which the data are to be processed or used are to be stipulated in concrete terms.

(1) § 28 sec. 1 No. 1 – for the purposes of a contractual or quasi-contractual relationship with the data subject

f.ex: employment agreement, membership, contract of sale

(2) § 28 sec. 1 No. 2 - in so far as this is necessary to safeguard justified interests of the controller and there is no reason to assume that the data subject has an overriding legitimate interest in his data being excluded from processing or use.

f.ex: personal data of employees in an M&A transaction

(3) § 28 sec. 1 No. 3 – if the data is generally accessible or the controller would be entitled to publish them, unless the data subject's legitimate interest in his data being excluded from processing or use clearly outweighs the justified interest of the controller.

f.ex: magazines, register, archives

(4) § 28 sec. 3 No. 3 – for purposes of marketing and advertisement if the data, compiled in lists or otherwise combined, concern members of a group of persons and are restricted to

- a) the data subject's membership of this group of persons,
- b) occupation or type of business,
- c) name,
- d) title,

- e) academic degrees,
- f) address and
- g) year of birth

and if there is no reason to assume that the data subject has a legitimate interest in his data being excluded from transfer.

German data protection law is constantly amended and adjusted to the requirements of changing circumstances. Therefore, provisions of the BDSG, also § 28 BDSG, are subject to reforms and it is highly likely that they will be changed in the upcoming years.

- Consent is only valid under certain conditions

§ 4a sec. 1 BDSG

*Consent shall be effective only when based on the data subject's **free decision**. He shall be **informed** of the purpose of collection, processing or use and, in so far as the circumstances of the individual case dictate or at his request, of the **consequences of withholding** consent. Consent shall be given **in writing** unless special circumstances warrant any other form. If consent is to be given together with other written declarations, it shall be made distinguishable in its appearance.*

The consent is revocable at any time. If the data subject has revoked its consent, all related data are to be deleted or blocked.

Additional requirements if data are transferred to the US:

The most important note for multinational companies with different affiliates is, that there is no such thing in German data protection law as an intra-group privilege for the transfer of data. Any transfer of personal data to another company, either part of the same group, partner, or random third party provider, requires sufficient legal permission or consent of the data subject as stated above. In addition to these requirements, the transfer of data to a non-EU country is subject to further restrictions.

- No transfer of personal data to countries with an inadequate level of data protection.

According to § 4b sec. 2 s. 2 BDSG, regardless of other legal permissions, the transfer of personal data shall not be effected in so far as the data subject has a legitimate interest in excluding the transfer. Such a legitimate interest is assumed if an adequate level of data protection is not guaranteed in the country the data is transferred to.

As the European Commission has decided that by default of a consistently stipulated data protection law, the US legal system does not provide for “sufficient guarantees” for data protection in terms of European data protection law.

However, under certain conditions, German data protection law deviates from this principle:

- Exceptions to § 4b sec. 2 s. 2 BDSG – Consent or performance of a contract

In connection with activities which fall in part or in their entirety within the scope of the law of the EU the transfer of personal data the US is admissible if

§ 4c sec. 1 No. 1 and 2 BDSG

- 1. the data subject has given his consent,*
- 2. the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request,*
- 3. the transfer is necessary for the conclusion or performance of a contract which has been or is to be entered into in the interest of the data subject between the controller and a third party,*
- 4. the transfer is necessary on important public interest grounds, or for the establishment, exercise or defence of legal claims,*
- 5. the transfer is necessary in order to protect the vital interests of the data subject,*

The most important stipulation is that the transfer of data to the US is admissible, if the transfer is necessary for the performance of a contract between the data subject and the controller. This comprises international monetary transactions and distance selling contracts for the sale of goods. Employment contracts can also constitute a contract in that sense. All transfers on the basis of § 4c sec. 1 No. 2 BDSG are however restricted by the condition, that the data transfer has to be essential for the purposes of the contract. The transfer of comprehensive data packages regardless of their provenance is hence not admitted.

If not under No. 2, transfers can also be legitimate if the data subject has expressed its consent with the transfer. It is, however, unlikely that the strict requirements of a valid consent are met in the majority of cases. The data subject has to be primarily informed about the risk of data transfers to countries without an adequate standard of data protection. Transparency with regard to security measures and data protection safeguards is hence necessary. Furthermore, the consent has to be based on the data subject's free decision. This is not complied with for example with regard to consent

expressed in employment contracts, as this is assumed to rather not be based on an entirely free decision.

- Exceptions to § 4b sec. 2 s. 2 BDSG – Adequate Safeguards

If none of the abovementioned exceptions apply, the transfer of personal data to the US is nonetheless possible, but it requires safeguarding measures of the companies involved to compensate for a generally inadequate standard of data protection:

§ 4c sec. 2 BDSG

[..] the competent supervisory authority may authorise individual transfers or certain categories of transfers of personal data to bodies if the controller adduces adequate safeguards with respect to the protection of privacy and exercise of the corresponding rights; such safeguards may in particular result from contractual clauses or binding corporate regulations.

(1) Contractual Clauses

The European Commission has developed a set of standard contractual clauses for the transfer of data to a third country. This Commission decision obliges all member states of the EU to recognize that companies that make use of unmodified EU standard clauses provide for an adequate level of data protection and can therefore transfer personal data to the US according to the basic data protection scheme (Consent of the data subject, § 4a BDSG or legal permission, § 28 BDSG).

The European Commission has also developed standard contractual clauses to use if the personal data are transferred to a processor in the US.

Alternatively, companies may use the standard contractual clauses of the ICC. Representatives of industry and commerce have criticized the EU standard clauses for being maladjusted to the needs of companies in the private sector. The ICC clauses have been approved by the European Commission and provide f.ex. for a facilitation of liability clauses in favour of an extension of intervention powers of the authorities. The ICC clauses on dispute settlement, auditing duties and responsibilities are regarded to be preferable for companies.

Apart from that, companies are always free to develop their own individual data protection clauses and to have them approved by the European Commission, if and so far as the parties have agreed in the contract to safeguard the principles of European and German data protection laws. The procedure of approval can be very tedious though.

(2) Safe Harbour Principles

The European Commission and the American government have elaborately discussed the issue of data transfer from the EU to the US. To simplify matters for the companies involved, they have agreed upon seven principles of data protection and the 15 so called “Frequently Asked Questions, FAQ”:

- **NOTICE:** Comprehensive duty to furnish information to the data subject
- **CHOICE:** The company must offer individuals the opportunity to choose (opt out) whether their personal information is to be disclosed to a third party.
- **ONWARD TRANSFER:** Transfer only if the principles of choice and notice are applied
- **SECURITY:** The company must dispose of adequate data security measures.
- **DATA INTEGRITY:** Transferred data must be relevant for the purposes for which it is to be used
- **ACCESS:** Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information
- **ENFORCEMENT:** Effective privacy protection must include mechanisms for assuring compliance with the Principles

If a company complies with the standards set forth in these principles, an “adequate standard of data protection” is sufficiently safeguarded and the company can therefore transfer personal data to the US according to the basic data protection scheme (Consent of the data subject, § 4a BDSG or legal permission, § 28 BDSG).

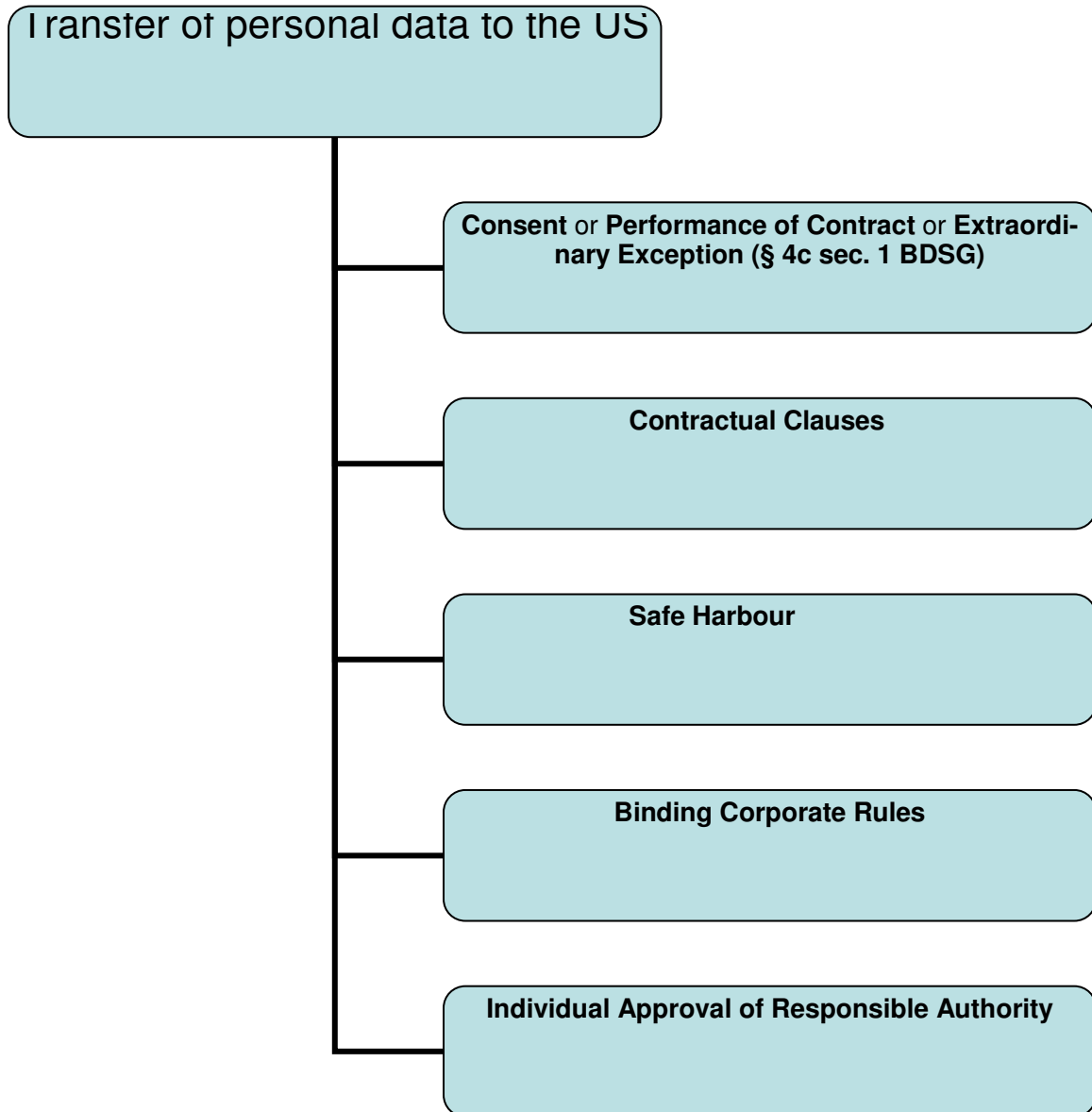
(3) Binding Corporate Rules

Within international groups of companies, so called “Binding Corporate Rules” are a common method of adequately safeguarding data protection standards. It is required and sufficient if the basic principles of European data protection law are adhered to. The European Commission has compiled a working paper in terms of the content of Binding Corporate Rules. It is though not yet decided, whether Binding Corporate Rules are subject to the approval of EU or member state authorities. To be safe, it is highly recommended to have one’s Binding Corporate Rules approved by the authorities until the legal status is clarified.

If the group operates companies in different member states, such an approval would necessitate every member state authority to accept the company's rules and would lead to an infinitely long procedure. An EU-wide approval system has not yet been established.

The ICC has developed a standard application form on the basis of the requirements of the aforementioned working paper to be used in all EU member states to facilitate matters.

Whichever path is taken, the approval requires the adoption of a global data privacy standard which is directly enforceable against the organisation by the individuals whose data are processed.



2. **When does German data protection law apply?**

- **Collection, processing and use of personal data on German territory by US-registered companies**

§ 1 sec. 5 BDSG

This Act shall apply in so far as a controller which is not located in a member state of the European Union or in another state party to the Agreement on the European Economic Area collects, processes or uses personal data in Germany.

Example:

US-company makes use of a German company to collect and store personal data of customers on a server within the territory of the European Union – German data protection law applies

- **US-parent company has subsidiaries in the Germany**

Example:

The subsidiary is located in Germany – German Federal Data Protection Act applies to the collection, processing and use of any personal data by the subsidiary in Germany.

- **Commissioned collection, processing or use of personal data**

Example:

A company's subsidiary in Germany makes use of a Processor to handle their data. If this Processor is located in the European Union as well, the transfer of personal data to the processor is not regarded to be "transfer" in the legal sense of the word. The Processor is regarded as being part of the subsidiary in this case and can collect, process and use personal data to the same extent as the subsidiary (with consent, § 4a BDSG or legal permission, § 28 BDSG)

If the Processor is located outside the European Union, f.ex. the US, the data exchange is regarded as "transfer" in the sense of the BDSG and therefore subject to the strict regulations on transfer of personal data to third countries as stated above.

C. Special Matters

- **Whistleblowing**

Example: A US company listed on a stock exchange has or plans on establishing subsidiaries in Europe. The company wants to apply its Code of Conduct also to the European employees.

The Sarbanes-Oxley Act (SOX) obliges US and foreign companies listed on US stock exchanges and their subsidiaries to establish independent internal audit committees and to provide opportunities for employees to make protected and anonymous disclosures in relation to accounting or financially relevant issues (“whistleblowing”). If a US company establishes subsidiaries in Germany and/or attempts to go into the German market, the SOX provisions are to be adhered to also with regard to subsidiaries and employees in Germany. The implementation of whistleblowing procedures is mostly accompanied by software based systems to allow for an efficient reporting system. Many companies additionally outsource the reporting function to a third party service provider using a confidential hotline or web service. Necessarily, this comprises the collection and processing of personal data of the alleged wrongdoer and the whistleblower himself and may also include the transfer of data to the parent company in the US. As German and European data protection law applies to such action effected on EU territory, the whistleblowing procedure has to be consistent not only with the SOX but also with German and EU data protection provisions. In most cases, it is not.

The French data protection agency (CNIL) ruled against McDonald’s and CEAC/Exide Technologies, prohibiting the implementation of the companies Codes of Conduct that provided for mandatory reporting of unlawful behaviour to the parent company in the US for infringement of data protection principles. The German Labour Court of Wuppertal ruled against WalMart also with regard to the implementation of a Code of Conduct in German branches of the company though concentrating mostly on labour law aspects of the matter. However, German data protection law has derived from European directives and therefore supposedly applies the same standards as the French authorities did.

Concerns have arisen in multinational US-based companies as the SOX and EU legislation seem to be in direct conflict. Companies subject to the SOX that fail to meet requirements related to effective whistleblowing may potentially face enforcement action or civil penalties by the US Securities and Exchange Commission (SEC) and can even be unlisted from the stock exchange. They may therefore tend to risk an infringement of European data protection law rather than not complying with the provisions of the SOX. There are however, possibilities to minimise the risks of infringement of EU data protection law while complying with the provisions of the SOX.

Recommendations:

- Implementation of whistleblowing procedures that adhere to both European and US legal requirements
 - (2) SOX compliance does not legitimate whistleblowing as such for it is not regarded as a “legal obligation” in the sense of Directive 95/46
 - (3) A whistleblowing system can be implemented for the purposes of a legitimate interest pursued by the controller
 - (4) Prompt notification to the person accused or reported on the details of the accusation, right to respond/contest or rectify information
 - (5) Keeping the collected personal data in the EU without transferring it to the US
 - (6) Implementation of appropriate cross-border transfer solutions
 - Consent of the individual reporting
 - Data protection agreement
 - EU model contracts
 - Safe Harbour Certificate
 - (7) Careful selection of processing agents
 - (8) Limiting or adjusting the reporting mechanism to required SOX provisions
 - Exempting EU based employees from the duty to report
 - Anonymous reporting as an exception

- **Cloud Computing**

Cloud Computing is a simple concept: Software and services such as e-mail, video or document sharing are accessed over the Web and through a browser. However, cloud computing raises difficult data protection issues.

Cloud computing relationships are technically complex and involve the transfer of data across multiple jurisdictions. Data are not simply processed but effectively transferred to a third party. The data change their physical location every other second from Germany to any other country, including the US. No one basically knows as to whether all servers used are efficiently secured, who has control over and insight to the data, who is therefore responsible to delete or block data, whether multiple single data can be assembled on another server to a complete new personal data, to the use and processing of which the data subject has never consented and the use and processing of which is neither covered by the purpose of a contractual relation.

According to European data protection law, as stated above, the transfer of data is subject to strict regulations. But with millions of possible third parties that control the data for a second, it is impossible have the adequate data protection level safeguarded. Pure cloud computing nearly infringes every principle of European data protection law:

- an individual has a right to know at any moment with whom and where what data is being stored or used.
- personal data must be kept for no longer than is necessary and must be accurate and up-to-date;
- personal data must be, at all times, kept secure and where processed by a third party be managed securely; and
- personal data should not be transferred outside the European Economic Area to any other country that does not have adequate protection for the rights of the individual.

Regardless of where the information is being processed, companies are challenged to take all reasonable steps to protect it from unauthorized uses and disclosures while it is in the hands of third party processors. The companies have to be satisfied that the third party has policies and processes in place, including training for their staff and effective security measures, to ensure that the information in its care is properly safeguarded at all times.

- **E-Discovery**

Example

Parent company in the US is subject to a trial and has to prepare the Discovery, data is needed from the German subsidiary that may have to object to the transfer of data due to local data protection law;

US companies with subsidiaries in the EU find themselves face another increasingly prominent conflict of US and European legislation related to discovery proceedings in US civil litigation. In “pre-trial discoveries” US firms are obliged to provide any information in their possession, custody or control upon request of the opponent if only the requested information is “relevant to any party’s claim or defence”. Even information that is not relevant in itself but may lead to the discovery of admissible evidence has to be provided as long as it is “reasonably likely” to be the subject of discovery in litigation.

Germany and most EU member states on the other hand have an inquisitorial legal tradition, leaving the decision as to what information is relevant for the trial to the judges. An obligation to submit documents to such an extent is unfamiliar to German law that also recognises obligations to store documents and data only sporadically, f.ex. in § 257 Commercial Code (*Handelsgesetzbuch – HGB*) and § 147 Fiscal Code (*Abgabenordnung – AO*).

Implemented by amendments to the U.S. Federal Rules of Civil Procedure (FRCP), which in effect added “Electronically Stored Information” as a new category of documents to provide for interrogatories, e-discovery demands include millions of emails, log files, electronic calendar entries, letters and other documents stored in electronic databases and can easily generate terabytes of information. Data that is stored with a company’s European subsidiary in the EU is mostly also regarded to be under the “control” of the US parent company and can therefore be subject to an e-discovery re-

quest. Conflicts may then arise, as the storage and the transfer of personal data, and the requested information is most likely to contain personal data, from the EU to the US is subject to strict regulations. Two issues are most crucial under German law

- Storage of data for the purpose of a potential obligation to disclose information in the course of e-discovery

In the absence of an expressive consent of the data subject, as it will most likely be the case in e-discovery matters, Sec. 28 of the Federal Data Protection Act (*Bundesdatenschutzgesetz-BDSG*) is the decisive provision with regard to the question, whether or not a company may collect, store and/or transfer personal data. Even if, ignoring the enormous logistical scope of such an endeavour, every data subject had expressed its consent in advance, this consent has to be revocable at all times. This requirement is inconsistent with US statutes, as employees can not opt out of having their documents examined during discovery proceedings.

Processing the data for the purpose of an e-discovery demand can only be permitted according to § 28 sec. 1 No. 2

“in so far as this is necessary to safeguard justified interests of the controller of the filing system and there is no reason to assume that the data subject has an overriding legitimate interest in his data being excluded from processing or use”

A legitimate interest in processing personal data is affirmed for safeguarding one's right in legal proceedings only, if the company arranges for adequate methods to store the necessary data on the one hand, but on the other hand respects the principles of data protection f.ex. through the implementation of a “Document Retention Policy”. Additionally, the different interests have to be balanced appropriately for every particular case. Data protection, with its principles of data reduction and data economy in Germany is highly valued by both courts and legislation, therefore it is highly unlikely that such a weighing of interest will result in favour of the admissibility of e-discovery.

- Transfer of data to the US

As a surplus, it is particularly difficult to justify the transfer of data to the US, as it is obligatory in an e-discovery demand. The transfer of data in this case is not subject to the provision of § 28 BDSG, as the United States are not recognized to have a “comparable standard of data protection”. The application of Safe Harbour Rules or EU model contracts cannot overcome this obstacle as the company should not rely upon its opponent to be part of Safe Harbour or enter into a contract with the EU subsidiary.

An exception to this rule is made however, for the purpose of safeguarding one’s interests in legal proceedings. The transferred data are then only to be processed within the limits of the purpose of their transfer, i.e. the particular proceeding. Under US law, however, all documents presented in a legal proceeding have to be made accessible upon request to the public.

German data protection law thus does not allow for the submittal of data to the United States in the course of an e-directory request.

US courts have proven to be rather reluctant with regard to multinational companies, whose European subsidiaries disagreed to submit documents with reference to local data protection laws, qualifying the statutes that restrict cross border disclosure as “blocking statutes”.

The Article 29-Working Party has recently considered the issue of the application of Directive 95/46/EC to the transfer of data outside of the EU for the purposes of pre-trial discovery obligations in the US. Again, the crucial point is that the data protection standard from a European point of view is not regarded as “comparable” to the European standard. The Working Party recommends however, that the first and major step towards a European acceptance of the disclosure would be to anonymize the transferred data and to negotiate with the courts as to a restricted disclosure of documents due to local data protection laws

Recommendations:

- Application of German data protection law in US civil proceedings
- Application for a “Protective Order”

- Legitimate transfer of data to the United States (Safe Harbour, EU model contracts)
- **US-Websites for EU market**

Example: Company outside in the United States runs a website, f.ex. a webshop that is accessible in the EU

Companies that run websites that collect and process data from its visitors, be it via the use of “cookies”, Java Script or online forms have long ignored EU data protection laws as they considered it to be inapplicable as long as the business beyond the website was located outside the EU territory. This assumption however, is false.

German data protection law is, according to the territoriality principle, applicable, if a US Company collects processes or uses personal data in Germany. The online offer of a company has already been ruled to be collection data “in Germany” if the offer is accessible from Germany and directed at German internet users.

Most companies underestimate that even though a website might neither be targeted to German or European internet users, they can be held liable for data protection law infringement, if they deploy “cookies” to gather and process personal data of European internet users. Those devices enable the company to control the personal computers of European Internet users. Thus, when these companies collect and process personally identifying data about an Internet user they are subject to European data protection law. [This interpretation of data protection provisions is supported by an Article 29-Work Group publication on the subject. This opinion is not unanimously shared.]

Specifically, they are subject to the data protection law of the Member State in which the Internet user’s computer is located.

Consequently, companies should, in order to avoid legal proceedings in Europe, adapt their compliance and data processing habits to the law of the EU and/or the member state they plan to direct their websites to.

To exemplify matters, companies with websites accessible from Germany have to comply with the following provisions:

- Given the absence of any actual physical presence in the EU, German law requires the company to have a representative within the EU, f.ex. a legal counsel or a DP-service agent, § 1 sec. 5 BDSG
- Personal data can only be collected or used upon consent of the data subject or within the limits of the German Telemedia Act [*Telemediengesetz-TMG*]. The latter imposes that personal data can only be collected or used, if it is essential for the purposes of a contractual relation between the data subject and the company.
- The data subject has to be informed as to how and for what purpose the collected data is collected, processed and used
- Infringements of these provisions can result in administrative fines of up to 50.000 €.

Useful links:

- **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**

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>

- **European Commission Standard Contractual Clauses for the transfer of data to third countries**

http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm

- **European Commission Standard Contractual Clauses for data processors established in third countries**

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:006:0052:0062:EN:PDF>

- **ICC Alternative Standard Contractual Clauses for data transfers to third countries**

<http://www.iccwbo.org/policy/ebitt/id20384/index.html>

- **ICC Standard Application form for the approval of Binding Corporate Rules**

<http://www.iccwbo.org/icciggb/index.html>

- **Useful information on Safe Harbour Rules**

<http://www.export.gov/safeHarbor/>

- **List of “Safe Harbour”- Companies**

<http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list>

July 2009

Axel Freiherr von dem Bussche, LL.M.
Rechtsanwalt, Partner
a.bussche@taylorwessing.com

Taylor Wessing
Partnerschaftsgesellschaft von Rechtsanwälten, Steuerberatern, Solicitors und Avocats à la Cour
www.taylorwessing.com