McDermott Will & Emery

Guide for International Counsel:

US Pre-Trial Discovery in Europe

July 2013 (Version 1)[1]

[1] Updates to this guide will be published on McDermott Will & Emery's website at www.mwe.com.

Table of Contents

Table of Contents

Introduction

Globalization and international trade bring European corporations and affiliates into contact with US markets. This may lead to US litigation, which differs significantly from litigation in most other countries of the world.

Increasingly, European corporations must handle US litigation discovery demands that require the production of evidence located in the European Union, in conflict with European and national privacy laws.

Notwithstanding conflicting obligations, there are ways to successfully navigate this legal maze. With advance planning and understanding, litigation risks can be controlled and mitigated.

This document provides guidance for lawyers and in-house counsel to properly satisfy their duties in relation to US discovery, without infringing European and national laws. Although the specific examples given relate to Germany, the situation is broadly similar across Europe.

Updates to this guide will be published on McDermott Will & Emery's website at www.mwe.com.

1. Pre-Trial Discovery in Civil Proceedings

It is worth beginning with a review of the most important aspects of US pre-trial discovery (discovery) when procuring evidence for US litigation in other countries. This section therefore focuses on civil proceedings in the US district courts (federal courts) that are governed by the Federal Rules of Civil Procedure (FRCP). Although the courts of the 50 US states and other territories have their own procedural rules, most do not differ significantly from the FRCP and will therefore not be considered further.

1.1. TRANS-BORDER DISCOVERY

Discovery is the stage in civil proceedings during which parties can obtain evidence from the opposing party by a variety of means. These include requests for admissions, written questions (interrogatories), subpoenas and other written requests for the production of documents and electronic information and depositions. Such means are unknown in civil code jurisdictions.

Discovery is based on the assumption that an extensive exchange of information between parties is the most efficient way to identify the issues in dispute whilst also eliminating any surprises at trial. In *Hickman v Taylor*, the US Supreme court emphasized:

> *Mutual knowledge of all relevant facts gathered by both parties is essential to proper litigation. To that end either party may compel the other to disgorge whatever facts he has in his possession.*[2]

Trans-border discovery is not limited to European companies that have been sued in the United States. It may also indirectly affect European affiliates of multinational companies if sister or parent companies are also parties to US litigation. US litigation typically starts with a complaint that has been duly served, which is then followed by months, if not years, of exchanging information and seeking information from third parties that is in some way relevant to the plaintiff's claims and defendant's defences.

1.2. SERVICE OF COMPLAINTS

Discovery proceedings basically require the concerned party to be subject to civil proceedings. Before a court can exercise personal jurisdiction over the defendant, he or she must be duly served with the complaint and summons. According to the FRCP, the summons and complaint must be filed with the court and then served upon the defendant. According to Rule 4(c) FRCP, "the plaintiff is responsible for having the summons and complaint served within 120 days". So-called process servers are often used to implement the service process and are particularly helpful if it is difficult to locate the defendant. Particular issues may arise if the defendant must be served outside the United States. These issues are discussed in the greater detail below.[3]

1.3. SCOPE OF DISCOVERY

1.3.1. GENERAL

Under the FRCP, the

> *[p]arties may obtain discovery regarding any non-privileged matter that is* ***relevant to any party's claim or defence****—including the existence, description, nature, custody, condition, and location of any documents or other tangible things and the identity and location of persons who know of any discoverable matter. For good cause, the court may order discovery of any matter relevant to the subject matter involved in the action.*[4] [authors' emphasis].

[2] US Supreme Court: *Hickman v Taylor*, 329 US 495, 501 (1947)
[3] Details: Section 2.
[4] Rule 26(b)(1) FRCP

US courts typically give "relevant" a very broad meaning. It has accordingly been ruled that "[d]iscovery should be allowed unless it is clear the information sought can have no possible bearing on the claim or defence of a party".[5] Any evidence, such as tangible items and data that might enable a defendant to better understand the subject matter of the case, or which might reasonably be useful for making a possible claim or preparing a defence, is therefore subject to discovery. The medium on which the data is held is irrelevant:

> *Documents or electronically stored information—including writings, drawings, graphs, charts, photographs, sound recordings, images and other data or data compilations—stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form.*[6]

Discovery therefore includes electronic documents and files, such as e-mails, but also hidden text, formatting codes, formulae, and other information associated with the file. These types of ancillary information are often known as metadata.[7]

1.3.2. LOCATION OF THE EVIDENCE AND ITS CUSTODY OR CONTROL

The territorial scope of discovery is not confined to US borders and the location of data is typically not important.[8]

In addition, FRCP Rule 34(a) simply refers to "the responding party's possession, custody, or control" of the evidence. It is therefore not even necessary that the party is actually in possession of the data, it is sufficient that it has "control" over the data.

In determining whether or not data is under the control of a party, the courts apply several criteria, such as the legal accessibility of the data or whether or not the data is regularly exchanged between the possessor and the party in the ordinary course of business. Even non-party affiliates of litigants may indirectly be subject to discovery requests. It has been decided that

> *A litigating parent corporation has control over the documents in the physical possession of its subsidiary corporation where the subsidiary is wholly owned or controlled by the parent corporation.*[9]

In *Alcan International v S.A. Day Manufacturing Co.,*[10] the defendant requested documents that were in the possession of the plaintiff's affiliate, situated in Germany. The court permitted the request, holding that the plaintiff had control over the documents of the German affiliate because the two entities were corporate members of a unified worldwide business under common control. The extent to which the gathering of evidence and data additionally requires the application of the Hague Convention is described below in Section 2.1.

1.3.3. LITIGATION HOLD

Information that might be subject to the discovery process must be preserved in advance of discovery. This duty begins as soon as it is reasonably foreseeable that the evidence would later be needed in court. It has been ruled that

> *The obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation.*[11]

A corporation is therefore obliged to preserve relevant information when it learns, or reasonably should have learned, of threatened or pending litigation. In order to comply with this obligation, the corporation must immediately inform employees who may have relevant information of their duty to preserve that information. This message, regardless of the manner in which it is communicated, is often referred to as a litigation hold request.

---

[5] *Sheldon v Vermont*, 204 F.R.D. 69 (D. Kan. 2011)
[6] Rule 34(a)(1)(A) FRCP
[7] See: The Sedona Conference (TSC)® Commentary on Ethics & Metadata March 2012 Public Comment Version
[8] *Anschuetz & Co., GmbH*, 838 F.2d 1362, 1364 (5th Cir. 1988); *Cooper Industries, Inc. v British Aerospace*, 102 F.R.D. 918, 919-920 (S.D.N.Y. 1984); *Quaak et al., v Klynveld Peat Marwick Goerdeler Bedrijfsrevisoren*, 2004 WL 415282 (1st Cir. 2004)
[9] *Uniden American Corp. v Ericsson Inc*. 181 F.R.D. 302 (M.D.N.C. 1998)
[10] *Alcan Int'l Ltd. v S.A. Day Mfg. Co., Inc.*, 176 F.R.D. 75 (W.D.N.Y. 1996)
[11] *Fujitsu Ltd. v Federal Express Corp*., 247 F.3d 423, 436 (2d Cir. 2001); *Mosaid v Samsung* (D.N.J. 2004) 348 F.Supp. 2d 332, 333; *Scott v IBM Corp*, 196 F.R.D. 233, 247 (D.N.J. 2000)

PRACTICE NOTE

Identifying when a litigation hold request must be sent is sometimes difficult to assess and requires a practical and legal understanding of the situation. Any destruction of data should therefore be preceded by a careful investigation of the situation, and document retention policies should reflect these high standards.

It has been decided that a corporation under an obligation to preserve documents "cannot blindly destroy documents and expect to be shielded by a seemingly innocuous document retention policy".[12] A party will only be excused in exceptional cases, such as when "electronically stored information [is] lost as a result of the routine, good-faith operation of an electronic information system" [13]

Any failure to comply with the litigation hold may result in severe sanctions. Document retention policies should therefore either explicitly provide for the retention of documents if the conditions of a litigation hold are likely satisfied, and any destruction of documents should be suspended.

1.3.4. LIMITATIONS OF DISCOVERY

It is advisable to know the different limitations of discovery because, if such limitations are applied properly, they may be used to limit access to evidence. The discovery of trade secrets or personal data may be prevented by protective orders. Attorney-client privilege and the work-product doctrine are among the most important limitations to discovery.

1.3.4.1. ATTORNEY-CLIENT PRIVILEGE

Attorney-client privilege provides a client with assurances that discussions with his or her counsel will not be disclosed to third parties. This privilege belongs to the client and only the client can waive it. Although there are minor variations from court to court, the requirements to establish the existence of attorney-client privilege are as follows:[14]

- The holder of the privilege is, or wants to become, a client.
- The person to whom the communication was made is a member of a bar, or the subordinate of someone who is a member of a bar, and is acting—in connection with this communication—as an attorney.
- The communication was made for the purpose of providing legal advice.

There are a number of exceptions to attorney-client privilege, the most important being that the client has waived the privilege.

PRACTICE NOTE

US courts typically take a narrow view of attorney-client privilege. In *Upjohn v US* it was ruled that

The privilege obstructs the search for the truth and because its benefits are, at best, indirect and speculative, it must be strictly confined within the narrowest possible limits consistent with the logic of its principle.[15]

It is therefore advisable to review the requirements of any attorney-client privilege on a case-by-case basis. This is of particular importance when analyzing communications with in-house or foreign attorneys or patent agents. Some US courts engage in a form of traditional choice of law "contacts analysis" when deciding whether attorney-client privilege also applies to attorneys in other countries.[16]

[12] *Lewy v. Remington Arms Co., Inc.*, 836 F.2d 1104, 1112 (8th Cir. 1988)
[13] Rule 37(f) FRCP
[14] *United States v United Shoe Machinery Corp.* 889 F. Supp. 357,85 USPQ 5 (D. Mass. 1950)
[15] Upjohn vs. US, 449 US 383 (1981)
[16] *Santrade, Ltd. v General Elec. Co.*, 150 F.R.D. 539, 545 (E.D.N.C. 1993); *SmithKline Beecham Corp. v Apotex Corp.*, No. 98-C3952, 2000 WL 1310668 (N.D. Ill. Sept. 13, 2000); In *Rivastigmine*, 237 F.R.D. zu 74 (S.D.N.Y. 2006)

1.3.4.2. WORK-PRODUCT DOCTRINE

The work-product doctrine is codified in Rule 26(b)(3) FRCP:

> *[A] party may obtain discovery of documents and tangible things otherwise discoverable under [Rule 26(b)(1) FRCP] and prepared in anticipation of litigation or for trial by or for another party or by or for that other party's representative […] only upon a showing that the party seeking discovery has substantial need of the materials in the preparation of the party's case and that the party is unable without undue hardship to obtain the substantial equivalent of the materials by other means.*

Among other things, the purpose of this doctrine is to protect an area of privacy in which a lawyer prepares and develops legal theories and strategies with a view to litigation. The protection afforded by the attorney work-product doctrine is far narrower than that of attorney-client privilege and essentially applies only to documents prepared by attorneys for their clients in anticipation of litigation or for trial. Moreover, as Rule 26(b)(3) FRCP provides, a party requesting an attorney's work product can, in some instances, be afforded access to the information if it is unable to obtain the substantial equivalent of the information by other means without undue hardship.

1.3.4.3. PROTECTIVE ORDERS

Protective orders prevent the disclosure of certain information under certain circumstances. Under Rule 26(c) FRCP, a party or any person from whom discovery is sought may move the court for a protective order. The motion often needs to include a certification that the person has, in good faith, conferred with other parties in an effort to solve the dispute without the court's assistance. The court may issue an order to protect a party from annoyance, oppression, undue burden or expense by

- Forbidding the disclosure or discovery of, or inquiry into, certain matters
- Designating persons who may be present while the discovery is conducted
- Requiring that a deposition be sealed and opened only on court order
- Requiring that a trade secret or other confidential research, development or commercial information not be revealed
- Requiring that the parties simultaneously file specified documents in sealed envelopes that have to be opened at the court's direction.

Protective orders can be applied as mechanisms to protect personal data. These are described in more detail in Section 3.

1.3.5. DISCOVERY INSTRUMENTS

1.3.5.1. DOCUMENT REQUESTS

Requests for documents are usually used to gather pertinent documents, such as contracts, employment files and billing records. As stated above, this also covers data stored electronically, the discovery of which has become known as electronic discovery or e-discovery. The request is made by serving a notice for document production after the parties have conducted a "meet and confer conference" to discuss, among other things, the discovery process.[17] Once a request for documents is made, the responding party must serve a written response within 30 days, unless the court orders differently.[18]

PRACTICE NOTE

It is recommended that potential issues with European laws, in particular privacy laws and blocking statutes, are discussed at the meet and confer conference.

[17] Rule 26(f) FRCP
[18] Rule 34(b) FRCP

1.3.5.2. DEPOSITIONS

Another common method of discovery is to take depositions, which are out-of-court statements given under oath by a party or any other witness.[19] Depositions may be used at trial or in preparation for trial and may be in the form of a written transcript, videotape or both. Usually depositions consist of an oral examination by the attorney for the company that served the deposition request, followed by an opportunity for all other parties to ask additional questions of the witness. Depositions enable a party to know in advance what a witness will say at the trial.

1.3.5.3. SUBPOENAS

In most cases, a subpoena is issued to compel a non-party to give testimony and produce documents that relate to the underlying litigation.[20] The list of documents and other items the subpoena deponent must to bring to the deposition is known as a *subpoena duces tecum*. These documents and other items are typically vital to the case and very often become numbered exhibits introduced at a trial.

1.3.5.4. INTERROGATORIES AND REQUESTS FOR ADMISSION

Interrogatories are written questions from one party to another. Interrogatories are intended to enable a party to learn the facts of the case and are used primarily to determine what issues are present in a case and how to frame a responsive pleading or deposition. The questions may be focused on any matter that is discoverable, *i.e.*, any matter not privileged that is relevant to the claims and defences of any party. The questions only need to be "reasonably calculated to lead to the discovery of admissible evidence".[21] The answers provided may be used as evidence at trial.

A request for admission is a request filed by one party in a lawsuit on another party in that lawsuit asking the second party to admit to the truthfulness of some fact or opinion. Both interrogatories and requests for admission simplify litigation by reducing the number and nature of the points in dispute.

1.3.6. SANCTIONS IN CASE OF DISREGARD

Any failure to comply with discovery duties can be sanctioned by the court. For example, the court may sanction a party if there has been actual suppression or withholding of the evidence. Such sanctions may include the following:[22]

- Directing that the matters embraced in the order, or other designated facts, be taken as established for purposes of the action, as the prevailing party claims
- Prohibiting the disobedient party from supporting or opposing designated claims or defences, or from introducing designated matters in evidence
- Striking pleadings in whole or in part
- Staying further proceedings until the order is obeyed
- Dismissing the action or proceeding in whole or only in part
- Rendering a default judgment against the disobedient party
- Treating as contempt of court the failure to obey any order except an order to submit to a physical or mental examination.

[19] Rule 30 FRCP
[20] Rule 45 FRCP
[21] Rule 26(b)(1) FRCP
[22] Rule 37 FRCP

2. International Legal Assistance

Service of the complaint and evidence-taking during litigation to be implemented in a non-US country may be subject to special rules of international assistance. Of particular importance are the Convention of 15 November 1965 on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters (the Hague Service Convention or HSC) and the Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters (the Hague Evidence Convention or HEC). The United States and Germany are both parties to these conventions.[23]

2.1. APPLICATION OF THE HAGUE SERVICE CONVENTION

The HSC is a multilateral treaty that allows service of process of "judicial or extrajudicial documents" from one signatory state to another without having to work through consular and diplomatic channels. According to the Preamble, the Convention is intended to create appropriate means to ensure that judicial and extrajudicial documents to be served abroad are brought to the notice of the addressee in sufficient time. It also improves the organization of mutual judicial assistance for that purpose by simplifying and expediting the procedure.

Service of a US complaint in Germany (without applying the HSC) would violate German law, even if service is permitted under US law. The usual US practice of hiring a process server who delivers a complaint and summons to the business address or domicile of the defendant could not happen in Germany.

The Hague Convention applies primarily to judicial documents that introduce judicial proceedings, such as the complaint brief. It also applies to a subpoena compelling a non-party to give testimony and produce documents. All other documents that are exchanged after introduction of the judicial proceedings during the normal course of things, such as requests for discovery, do not necessarily have to be served in line with HSC proceedings.[24]

2.1.1. THE UNITED STATES

According to the delegates of the Hague Conference, the HSC applies exclusively to documents served abroad. This is reflected in Article 1 HSC, which provides that the Convention "shall apply in all cases, in civil or commercial matters, where there is occasion to transmit a judicial or extrajudicial document for service abroad". Rule 4(f) FRCP explicitly refers to the HSC if a complaint needs to be served outside the United States. Nevertheless, the HSC is not mandatory in all cases where a foreign defendant is involved.[25]

2.1.1.1. AGENT FOR SERVICE

If the complaint is filed against a foreign company, it can also be served upon its legal representatives, such as its officers, *i.e.*, the Chief Executive Officer (CEO), managing or general agents or any other agent authorized by appointment or by law to receive service of process.[26] This means a complaint can be duly served upon a foreign defendant through its CEO, provided he or she is on US territory. Whether and to what extent the HSC is applicable has been specifically assessed by the US Supreme Court in *Volkswagen AG v Schlunk*.[27] Subject to that decision was the question of whether or not a subsidiary situated in the United States can be used as a so-called agent for service on behalf of a defendant situated in the European Union without applying the Convention. The US Supreme Court concluded that "where service on a domestic agent is valid and complete under both state law and the Due Process Clause, our inquiry ends and the Convention has no further implications." The subsidiary of the defendant, and even its (directing) employees, could therefore represent agents for service. They can be used as regular addressees for service, in which case it would not be necessary to implement service on the basis of the HSC.

2.1.1.2. DEFENDANT'S US COUNSEL

The lawyer of a non-US defendant is also an appropriate addressee for the complaint.[28] A motion to dismiss for insufficient service of process may therefore challenge the plaintiff to use the defendant's counsel as the addressee to make service by alternate means.[29]

---

[23] 20 UST. 361
[24] *Black/Lange*, Civil Litigation, p. 27; *Hollmann*, RIW 1982, 784, (788); *Wölki*, RIW 1985, 530, (533); BT-Drs. 7/4892, S. 48
[25] *Volkswagen AG v Schlunk*, 486 US 694, 108 S. Ct. 2104, 100 L. Ed. 722 (1988)
[26] Rule 4(e) FRCP
[27] *Volkswagen AG v Schlunk*, 486 US 694, 108 S. Ct. 2104, 100 L. Ed. 722 (1988)
[28] *Richmond Technologies, Inc. v Aumtech Business Solutions*, No. 11-CV-02460-LHK, 2011 WL 2607158 (N.D. Cal. July 1, 2011), and *Gramercy Insurance Co. v Kavanagh*, No. 3:10-CV-1254-D, 2011 WL 1791241 (N.D. Tex. May 10, 2011).
[29] Rule 4(f)(3) FRCP

PRACTICE NOTE

The service of the complaint through HSC proceedings might be beneficial for the defendant because the service of process via the HSC typically takes longer than direct service on US territory. The discovery phase would consequently start later, giving more time to prepare and organize the tasks that follow discovery.

Non-US corporations that already know they have been sued in the United States, or believe there is a probability of being involved in US litigation, should therefore weigh up the pros and cons before sending employees, who run the risk of being served, to the United States.

2.1.2. GERMANY

Even though the Convention offers plaintiffs a number of channels through which the service can be accomplished, the German authorities have limited the scope of its application.

2.1.2.1. INVOLVEMENT OF THE CENTRAL AUTHORITY

The service of a US complaint must, in most cases, be carried out by filing a request with the Central Authority,[30] requesting either a compulsory service or an informal, voluntary service.[31] In Germany, each of the 16 Federal States (Länder) has its own Central Authority.

At present, complaints cannot be served by post, e-mail or fax. In addition, and with the exception of US citizens, complaints cannot be served on German nationals through US diplomats.[32] Furthermore, judicial officers cannot be employed for the service, *i.e.*, German lawyers, detectives, policemen or any private service providers are not empowered to serve a complaint under German law. Depending on the method of service employed, the complaint may then be transmitted by the Central Authority to a court bailiff, a registrar of the court or a postman who serves the complaint.[33]

2.1.2.2. TRANSLATION REQUIREMENTS UNDER GERMAN LAW

Germany requires an official translation into German of the document(s) to be formally served pursuant to Article 5(1) or Article 10(b)/(c) HSC.[34] Enclosures annexed to the documents must also be translated into German.[35]

PRACTICE NOTE

Translations often render the service of process burdensome and costly. For example, in patent litigation reference must be made to a patent and sometimes to prior art documents that are not always available in German. The judicial document initiating the proceedings could be drafted in a way to avoid the inclusion of (too many) translations, as long as this does not render the service incomplete.[36] This should, however, be done in co-operation with German counsel who understand the legal limits. Counsel to defendants, should carefully assess whether or not the document is complete when it is served. An incomplete document may give reason to refuse service.

2.1.2.3. SERVICE OF SUBPOENAS IN GERMANY

Residents or citizens of the United States located in Germany must be responsive to US subpoenas served upon them.[37] There are no provisions for service upon non-US nationals or residents. The service of a subpoena in Germany would, in any event, have no coercive effect. This may be the reason why they are not routinely served upon witnesses living in Germany.

2.2. APPLICATION OF THE HAGUE EVIDENCE CONVENTION

[30] Article 5 HSC
[31] This type of service requires that the addressee accepts the service.
[32] Except for US citizens
[33] Section 4 (1) AusfG, Article 5 Abs. 1(a) HSC
[34] BGBl 1979 II, S. 779
[35] Article 5 (3) HSC; see *Jayme/Hausmann, Internationales Privat- und Verfahrensrecht*, (2009), *Haager Übereinkommen über die Zustellung gerichtlicher und außergerichtlicher Schriftstücke im Ausland in Zivil- oder Handelssachen* - HZÜ, Art. 5 HZÜ N° 6.
[36] With respect to the limits see German Federal Supreme Court, NJW 2007, 775 (for the European law concerning services)
[37] 28 USC. Section 1783, R. 45 (b)(29 FRCP

2.2.1. THE UNITED STATES

In *Aerospatiale*[38], the Supreme Court held that the application of the HEC is neither mandatory nor exclusive. The Supreme Court adopted a rule of comity. The application of the HEC therefore depends on the facts of each case, the sovereign interests involved and the likelihood that resorting to the Hague Convention will be effective. The US Supreme Court identified five factors to be taken into consideration during the analysis:

1. The importance of the documents or information requested for the litigation
2. The degree of specificity of the requests
3. Whether or not the information originated in the United States
4. The availability of alternative means of securing the information
5. The extent to which noncompliance with the requests would undermine important interests of the United States or the state where the information is located.

In construing *Aerospatiale*, the courts have created two additional factors to consider: [39]

1. The good faith of the party resisting discovery
2. The hardship of compliance on the party or witness from whom discovery is sought.

US courts applying these balancing tests clearly tend to prioritize discovery over non-US law. As such, US litigants typically do not have to resort to the HEC before seeking discovery against non-US litigants under the FRCP. As soon as there is a party to the litigation, and provided the court has jurisdiction over it, the party is obliged to produce evidence that is within its control.[40] The HEC does not, therefore, deprive a US District Court of jurisdiction to order production of evidence located abroad.

This means the HEC is not applicable if the evidence (data, documents, *etc.*) is "transportable" to the United States (procurement of evidence from abroad). However, a procurement of evidence in a non-US state (such as investigations/depositions to be carried out on German territory) requires that the proceedings of the HEC must be followed.[41]

2.2.2. GERMANY

2.2.2.1. PRODUCTION OF DOCUMENTS

German authorities are willing to assist the taking of evidence on behalf of US courts. Germany has, however, filed a reservation under Article 23 HEC:

> *A Contracting State may at the time of signature, ratification or accession, declare that it will not execute Letters of Request issued for the purpose of obtaining pre-trial discovery of documents as known in Common Law countries.*

Accordingly, letters of request pertaining to "US pre-trial discovery of documents" will not be carried out by the German authorities. This includes electronically stored documents, so e-discovery cannot be enabled through the HEC.

There is discussion in Germany as to whether this reservation excludes all requests for pre-trial discovery of documents or permits narrowly drafted requests limited to the production of specific documents. In support of the latter view, it is argued that the aim of the reservation is to prevent "fishing expeditions". Nevertheless, the German authorities do not execute any request that is focused on the discovery of documents. This strict approach has been confirmed by the German courts.[42]

---

[38] *Societe Nationale Industrielle Aerospatiale v United States*, 482 US 522 (1987)
[39] *Richmark Corp. v Timber Falling Consultants*, 959 F.2d 1468, 1475 (9th Cir. 1992)
[40] *Anschütz & Co. v Mississippi River Bridge Authority*, 474 US 812 (1985); *Messerschmitt Bolkow Blohm v Virginia Walker, et al.*, Amicus Curiae Brief der USA, 25 I.L.M. 803 (1986)
[41] *Volkswagen AG v Falzon*, 461 US 1303 (1983). this decision is an exception.
[42] Appeal Court Celle, July 2007, 16 VA 5/07; Appeal Court Munich, Decision of 27 November 1980, 9 VA 3/80

2.2.2.2. DEPOSITIONS

Article 23 HEC explicitly refers to "pre-trial discovery of *documents*" [authors' emphasis]. Germany's reservation therefore prevents document discovery but does not exclude other forms of discovery, such as witness testimony through depositions. A witness could even be asked to testify about the content of a certain document if the document is identifiable and designated in the request. Such testimonies could involve the witness bringing particular documents to the deposition hearing, but not being obliged to hand them out. The advantage of the HEC is that judicial compulsion can be applied if the witness is not willing to testify. Requests for evidence are submitted directly by the US court to the appropriate regional German Authority, which then selects the competent court in front of which the witness will be deposed.[43]

PRACTICE NOTE

The request for undertaking a witness deposition in front of a German court is typically drafted by US counsel, who submit it to the US court on behalf of which the German authorities will be providing legal assistance. After granting approval, the US court sends the request to the competent German Central Authority.

The deposition will later be directed by a German judge of a lower instance court (Amtsgericht). Unlike in the United States, the German judge will play an active role during the deposition. Typically, German Amtsgericht judges are not familiar with US law, tend to obtain their knowledge of the case only through the content of the request and often apply their own local standards to the deposition. It is therefore advisable to involve German counsel during the drafting of the request to render the deposition as exhaustive as possible.

A well-prepared request that provides the framework and limits of the deposition is likely to be highly beneficial. German counsel can help to identify what are admissible and inadmissible questions, in order to avoid a charge of being on a fishing expedition. In addition, German counsel can monitor communication with the relevant Central Authority and the German court to increase the speed of the process. In some cases that have been managed by German counsel, it has been possible to get a date for a deposition only a few weeks after filing the request.

The witness is often willing to testify without the necessity of compulsion. It is then frequently asked if, in such a situation, the HEC procedure could be circumvented. In order to answer this, it is useful to know that a bilateral agreement between the United States and Germany relating to the taking of evidence[44] requires that

- No compulsion is used
- The voluntary deposition takes place at the US Consulate
- The deposed person has the opportunity to be accompanied by legal counsel.

Even for voluntary depositions, permission from the German authorities (the German Ministry of Justice) is still required.

To get the process started, the US Consulate must be informed in advance about the deposition. Once the deposition request is made, the US Consulate asks the US Embassy in Berlin to approach the German Ministry of Justice to obtain approval for the deposition. Voluntary depositions can then be carried out at the US Consulate in Frankfurt.

[43] For Germany, see list in the Federal Law Gazette: BGBl 1995 II, S. 77.
[44] See bilateral agreement relating to the taking of evidence: exchange of notes at Bad Godesberg and Bonn 11 February 1955, 13 January and 8 October 1956; agreement relating to the taking of evidence: exchange of notes at Bonn 17 October 1979 and 1 February 1980.

PRACTICE NOTE

Parties are frequently tempted to organize depositions in Germany without involving public authorities. The German Government is of the opinion that this constitutes a violation of German jurisdictional competency. This is the case even if the witness is willing to testify voluntarily. Several commentators are even of the opinion that obtaining a deposition not authorised by the Central Authority constitutes a criminal offence under Section 132 of the German Criminal Code.

As it has not yet been clarified by German courts whether the deposing of a witnesses may (or may not) be sanctioned by penalties, it is advisable to follow the HEC procedure outlined above, which is not necessarily time consuming. Even a deposition under the HEC can be implemented in a few weeks.

FIGURE 1: US DISCOVERY IN GERMANY

Legal Basis	Content	Characteristics
The HEC	Procurement of evidence on German territory, except documentary discovery	Compulsion possible Evidence taken in front of a German court
Exchange of Notes at Bad Godesberg (Bilateral Agreement)	Depositions	Compulsion not possible At the US Consulate with the involvement of the German Ministry of Justice
FRCP (without application of the HEC)	Procurement of evidence from Europe/Germany	Available as soon as the party has control over evidence located in Germany

3. Privacy Laws

3.1. DATA PROTECTION IN THE UNITED STATES

The United States is dominated by a "sectoral approach" to data protection. It relies on a combination of legislation, regulation, and self-regulation. To date, there is no single data protection law in the United States comparable with the European Union's Data Protection Directive[45] (the Directive). Although some sectors provide for data protection, at least in part, *e.g.*, the Fair Credit Reporting Act and the 2010 Massachusetts Data Privacy Regulations, most do not.

3.2. EUROPEAN FRAMEWORK

The European framework is mainly based on the Directive, which was established to provide a regulatory basis to guarantee secure and free movement of personal data across the national borders of EU Member States. It sets a standard of security around personal data, wherever it is stored, transmitted or processed. The Directive defines the basics rules of data protection that Member States were required to transpose into the national laws by which each EU Member State individually manages the regulation and enforcement of data protection within its jurisdiction.

EU directives typically award Member States discretion as to the rules to be adopted. Often directives just set minimum standards and require particular legislative measures to transpose the provisions of the directive into national law. The Court of Justice of the European Union has, however, recently ruled that Member States are not allowed to make processing of personal data subject to conditions in addition to those outlined in the Directive.[46] The Directive rather provides for full harmonization and this, basically, eliminates the discretion of the Member States and significantly reduces the differences between them. There are still some (minor) differences between the Member States, for which reason the European Union is presently projecting the establishment of a Data Protection Regulation, which will be self-executing and accordingly will not require any implementing measures. The following chapters, however, mainly refer to the Directive and not to national data protection law.

3.2.1. INTERFERENCES WITH DISCOVERY

3.2.1.1. PERSONAL DATA

The main interference with discovery is the restriction the Directive places on the processing of "personal data". Personal data is broadly defined as "any information relating to an identified or identifiable natural person" and "processing" represents broadly "any operation or set of operations which is performed upon personal data, whether or not by automatic means."[47] Accordingly, almost all operations in relation to personal data occurring during different stages of US litigation, such as the retention, storing, screening (culling), disclosure, onward transfer and secondary use of data, are relevant and necessarily require a legal basis. The Directive is based on the concept that consent is generally legally required for the collection and processing of data. In certain circumstances, however, data can be processed without consent.

Personal data may only be kept for the period of time necessary for the purposes for which the data have been collected, or the period of time during which they are further processed. Article 6 of the Directive provides that personal data must be processed fairly and lawfully, collected for specified, explicit and legitimate purposes and not used for incompatible purposes. Any retention, preservation, or archiving of data for the purpose of a litigation hold would amount to processing and may only be justified if it is permitted by the Directive. In other words, the processing of personal data is prohibited unless it has been explicitly permitted. For this reason, data controllers in the European Union are not entitled to store personal data at random for an unlimited period of time because of a vague possibility of litigation in the United States.

3.2.1.2. LEGITIMACY OF PROCESSING PERSONAL DATA FOR LITIGATION PURPOSES

The processing of personal data for the purpose of pre-trial discovery must be legitimate, *i.e.*, it must satisfy one of the grounds set out in Article 7 of the Directive. Similar legal provisions can be found in national laws.[48] Transfers of data to the United States must meet the requirements of Article 26 of the Directive. For the purposes of the Directive, the United States is a "third country" [49] and therefore special requirements must be fulfilled in addition to the general consent required for the

[45] Directive 95/46 of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data.
[46] European Court of Justice (ECJ) judgment in joint cases C-468/10 and C-469/10
[47] Article 2(b) Data Protection Directive (the Directive)
[48] For the German law: Sections 28(1) and (2) of the German Data Protection Act (BDSG)
[49] Any country other than the EU and European Economic Area (EEA) Member States

processing of personal data. Analysis on two levels is required. The first level of the analysis is discussed below in Sections 3.2.1.2.1. and 3.2.1.2.2, and the second level of the analysis in Section 3.2.1.2.3.

For the first level of analysis, the grounds indicated in Article 7 of the Directive are of particular importance. The two grounds that possibly justify the processing of personal data in connection with US litigation are

- Consent of the "data subject"[50]
- A legitimate interest pursued by the controller or by the third party to whom the data are disclosed under Article 7(f).

3.2.1.2.1. CONSENT

According to Article 2(h) of the Directive, the data subject's consent is

> *Any freely given specific and informed indication of his* [the data subject's] *wishes by which the data subject signifies his agreement to personal data relating to him being processed.*

The data exporter in the European Union must also be able to produce evidence of the data subject's consent. It is required to demonstrate that the data subject was adequately informed. The data subject must also be given a real opportunity to withhold his or her consent without suffering any penalty, or to withdraw it if he or she has a change of mind.

In most cases it is difficult to get such "informed consent" from all relevant data subjects. The data subjects can be customers or competitors of the company and the controller might feel uncomfortable asking these people for consent. The time frames given under the discovery are often too narrow to obtain consent from a plurality of data subjects. It is particularly challenging to fulfill these high standards with respect to employees, owing to their contractual relationship with the controller.

3.2.1.2.2. NECESSARY FOR THE PURPOSES OF LEGITIMATE INTERESTS

According to Article 7(f) of the Directive, personal data can also be processed if it is necessary "for the purposes of the legitimate interests pursued by the controller or by the third party". Compliance with the duties of discovery may be found to be sufficient for the purposes of such legitimate interests. The provision requires that these interests are not "overridden by the interests for fundamental rights and freedoms of the data subject".

BALANCING THE INTERESTS OF THE CONTROLLER AND DATA SUBJECT

On one hand, the discovery process is aimed at preserving and producing data that is potentially relevant to the litigation. Each party gets access to the data that is necessary to support its claim or defence, with the goal of ensuring fair proceedings. Parties face strict penalties if they fail to comply with discovery demands.

On the other hand, the interests of the data subject must be considered, *i.e.*, his or her fundamental rights and freedoms have to be weighed against the aims of discovery. The balance of interests necessitates taking into account issues of proportionality, the relevance of the personal data for the US lawsuit, the sensitivity of the data for the data subject and the consequences of its disclosure for the data subject. This is reflected in Article 6 of the Directive, which provides that personal data shall be fairly and lawfully processed, collected for specified, explicit and legitimate purposes and not used for incompatible purposes. Adequate safeguards therefore have to be put in place.

The discovery demand is often focused on large data sets. In order to adequately consider the interests of the data subject, the data set must first be filtered or culled. The filtering activity should preferably be carried out in the country where the data are kept, possibly by a trusted third party, to determine which data are personal before the data is transferred to the United States. There are various stages to this filtering activity, including determining the information that is objectively relevant to the issue being litigated in the United States, then moving on to assessing the extent to which this includes personal data. This activity results in a much more limited set of personal data. The controller must also proactively exploit the legal possibilities that are allowed under US procedural law to solve emerging conflicts between discovery and the interests of data subjects. Such legal possibilities are described in the International Principles of The Sedona Conference (TSC)®.[51]

[50] Article 2(a) Data Protection Directive: A data subject is"an identified or identifiable person to whom the personal data relate."
[51] See Section 3.3.

PRACTICE NOTE

Familiarity with electronic data discovery is crucial to conducting internal investigations efficiently, as well as to quickly and economically identifying electronically stored information in case of litigation. It often transpires that parties to a lawsuit do not have sufficient knowledge about electronic records management practices or their legal obligations when they are served with a discovery request. This suggests that preparatory measures, such as the establishment of suitable data records management policies, should be taken well in advance of any litigation.

SENSITIVE PERSONAL DATA

Higher legal thresholds are applicable where the data contains sensitive personal data.[52] Processing sensitive personal data requires either explicit consent from the data subject (Article 8(a)) or assurances that the processing is necessary for the establishment, exercise or defence or legal claims under Article 8(e).

TRANSPARENCY AND RIGHTS OF THE DATA SUBJECT

When processing personal data for the purpose of US litigation, Articles 10 and 11 of the Directive need to be taken into account. These provisions concern the issue of what information should be provided to the data subject. Typically, this requires a general advance notice indication that personal data might be processed for US litigation. As soon as the data is actually processed, a further notice should be issued setting out the identity of the recipients of the data, the purposes of the processing and the categories of data concerned. The data subjects should also be informed about their rights—such as the right to object to the processing of their data on compelling legitimate grounds relating to that person's particular situation—if the processing is to be legitimate according to Article 7(f). The only exception is if there is a substantial risk that such information would jeopardize the ability of the litigant to properly investigate the case or gather the necessary evidence.[53]

Article 12 of the Directive gives the data subject the right to have access to the data held about him or her. The data subject may check the accuracy of the data and rectify it if it is inaccurate, incomplete or outdated.

The data controller must ensure that the individual's rights are upheld prior to the transfer. This duty can be imposed on the party receiving the data by means of a Protective Order.

DATA SECURITY

The data controller must take all reasonable technical and organizational measures to preserve the security of the data. The data must be protected from accidental or unlawful destruction, accidental loss and unauthorized disclosure or access. These duties are also imposed on the law firms and litigation support services involved in the litigation, including and any other entities involved in the collection or review of the information.

3.2.1.2.3. TRANSFERS OF DATA TO THE UNITED STATES (2ND LEVEL OF THE ANALYSIS)

A transfer of personal data to a non-EU country that does not ensure an "adequate level of protection" as required by Article 25 of the Directive is prohibited, even if the requirements of the legal basis described in Section 3.2.1.2.2 are satisfied. The European Commission has the power to determine, on the basis of Article 25(6) of Directive, whether or not a third country ensures an adequate level of protection through its national laws or the international commitments into which it has entered. Where the Commission finds that a third country does not ensure an adequate level of protection, any transfer of personal data to that third country is prohibited.[54]

According to the European Cmmission, the United States is a third country that does not principally ensure this level of protection. Any transfer of data to the United States is therefore prohibited. Provided the processing is in compliance with the requirements of the analysis on the 1st level, there are four exceptions to the basic prohibition on the 2nd level of the analysis:

1. Personal data can be transferred to an entity established in the United States that has subscribed to the **Safe Harbor Program**.

[52] Article 8 of the Directive
[53] Article 29 Data Protection Working Party: WP 158 - Working Document 1/2009 on pre-trial discovery for cross border civil litigation, adopted on 11 February 2009
[54] Article 25(4) of the Directive

2. Personal data can be transferred to a recipient in the United States that has entered into a transfer contract with the data exporter by which the latter adduces adequate safeguards. The **standard contract clauses** issued by the European Commission in its Decisions of 15 June 2001 or 27 December 2004 can be used for that purpose.

3. The recipient has established a set of **binding corporate rules** (BCRs) that have been approved by the relevant data protection authorities.

4. **Last resort**: A further possible ground for processing the data for the purpose of US litigation is provided by Article 26(1)(d) of the Directive: "The transfer is necessary or legally required on important public interest grounds, or for the *establishment, exercise or defence of legal claims*" [authors' emphasis].

SAFE HARBOR

The US Department of Commerce, in consultation with the European Commission, developed a Safe Harbor framework that provides a mechanism for US entities to reach an adequate level of protection of personal data. A corporation that decides to participate in the program must comply with the US-EU Safe Harbor Framework's requirements and publicly declare that it adheres to the seven Safe Harbor Privacy Principles listed on the website of the US Department of Commerce.[55] This self-certification must be repeated annually in writing. Participating organizations are deemed to provide "adequate" privacy protection.

PRACTICE NOTE

Safe Harbor self-certification is a very quick process. It can be implemented in several days and no further approvals from national data protection authorities for data transfers will be necessary. It should, however, be taken into account that the Safe Harbor program can only legitimize data transfers from the controller to the US entity certified under the program. Onward transfers to the adverse party or the US courts are therefore still not permitted.

The program may, however, allow a Safe Harbor-certified entity to undertake operations in the United States on a bigger data set. This could include the reviewing, filtering and culling of the data set with the aim of reducing it to only the data relevant to the US litigation. A legitimate ground must still be found for the onward transfer of the resulting reduced data set.

STANDARD CONTRACTUAL CLAUSES

Standard contractual clauses offer sufficient safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and the exercise of those rights. By incorporating standard contractual clauses into a contract, personal data can flow from a data controller established in any of the 27 EU Member States and three European Economic Area (EEA) member countries (Iceland, Liechtenstein and Norway) to a data controller established in the United States. Two sets of standard contractual clauses have been adopted for transfers between data controllers[56] and one set exists for transfers between a data controller and a data processor.[57]

The standard contractual clauses are considered as sufficient safeguards in light of the applicable data protection rules. If they are used unmodified, they are not subject to approval by the national data protection authorities. Some national authorities require a copy of the contract so they can check whether or not the document corresponds to the European Commission's standard contractual clauses.

[55] http://export.gov/safeharbor/eu/eg_main_018365.asp
[56] First model: 2001/497/CE and second model: 2004/915/CE
[57] European Commission Decision 2010/87/EU, 2010 O.J. (L 39) 5-6, 11 (EU)

PRACTICE NOTE

The standard clauses do not require approval from national data protection authorities and so can be established quite quickly. It should be taken into account, however, that they can only legitimize data transfers between the contracting parties. Onward transfers to the adverse party or the US courts are not legitimised through standard clauses.

Nevertheless, like the Safe Harbor Program, standard clauses may allow for reviewing and filtering the data sets with a view to culling the data not relevant to the US litigation to be undertaken in the United States. A legitimate ground must still be found for the onward transfer of the reduced data set.

BINDING CORPORATE RULES

BCRs form an international code of practice and policy followed by companies belonging to the same multinational corporation. BCRs are useful to companies that frequently export personal data from the EEA to other group entities located in third countries that do not ensure an adequate level of protection, such as the United States. BCRs are an alternative to standard contractual clauses if it is too burdensome to sign such clauses for each transfer made within a group. BCRs must, however, be approved by the relevant national data protection authorities pursuant to their own national legal procedures.

PRACTICE NOTE

Establishing a BCR for the purpose of solving data protection conflicts in on-going US litigation would typically not comply with the time constraints of the US discovery process. It would probably take too much time for group companies to internally agree on the policy and the BCR to be approved by the national data protection authority. In addition, it has to be taken into account that a BCR could only legitimize data transfers within the group, so transfers to the adverse party or the US courts would still not be permitted. Nevertheless, a BCR could be a valuable element in a data protection policy, implemented well ahead of any US litigation, and may include suitable data records management mechanisms in case of a litigation hold.

LAST RESORT

Article 26(1)(d) of the Directive allows a data transfer provided it is "necessary or legally required for the establishment, exercise or defence of legal claims". It is typically accepted that the fulfillment of discovery demands falls under this provision. Nevertheless, the data protection authorities give a very narrow interpretation of this provision so it must be understood as being a last resort.

The transfer must still first comply with the requirements of the analysis on the first level as outlined in Section 3.2.1.2.2. This includes a balance of the relevant interests that takes into account issues of proportionality, the relevance of the personal data for the US lawsuit, the sensitivity of the data for the data subject and the consequences of its disclosure for the data subject. In particular, it must be ensured that "interests for fundamental rights and freedoms of the data subject"[58] are not overridden.

From the balance of interests, it follows that the controller must first apply all reasonably available legal, organizational and technical measures to safeguard the data subject's rights before reference can be made to Article 26(1)(d) of the Directive. In other words, the legitimacy of the transfer requires an exhaustion of the protective means that are available under US law, for instance the International Principles of TSC®.[59] If, after taking all possible protective measures, it is in the interests of the data subjects for the transfer not to occur, the transfer will not be allowed. This does, however, seem to be the exception.

[58] Article 7(f) of the Directive
[59] See section 3.3

FIGURE 2: REQUIREMENTS FOR PROCESSING PERSONAL DATA FOR THE PURPOSE OF US LITIGATION

1st Level of the Analysis	
Is informed consent of the data subject available? Informed consent allows the processing and transfer of data without further analysis on the 2nd level.	Legitimate interests of the controller or a third party, which are not overridden by the fundamental rights and freedoms of the data subject: Balance of interests in consideration of proportionality!

2nd Level of the Analysis			
Safe Harbor Certification	Standard Contractual Clauses	Binding Corporate Rules	Last resort
Allows transfers to certified company. No onward transfer to US courts/adverse party!	Allows transfers to contract partner. No onward transfer to US court/adverse party!	Allows transfers within the group. No onward transfer to US court/adverse party!	Onward transfer to US court/adverse party is possible provided all measures to safeguard the data have been taken and there are no overriding interests of data subjects; see 1st level of the analysis.

3.2.1.3. DATA MANAGEMENT POLICIES

Data management policies that provide for retention periods in compliance with national legal requirements might be helpful for reducing the amount of data. Of course, such policies can only be applied if the data are not necessary for specific or imminent US litigation, in which case the data management policy must be suspended and data must be retained until the conclusion of the proceedings.

3.2.1.4. EXTERNAL SERVICE PROVIDERS

Where external service providers are used, e.g., litigation support companies, as part of the litigation process, the data controller would still remain responsible for the resulting processing operations as those providers would typically be acting as processors within the meaning of the Directive. External service providers, who must be appointed by contract, must also comply with the principles of the Directive. They must ensure that the information is collected and processed in accordance with the principles of the Directive, and that the information is only processed for the specific purposes for which it was collected. In particular, they must abide by strict confidentiality obligations and communicate the information processed only to specific persons.

3.3. INTERNATIONAL PRINCIPLES OF THE SEDONA CONFERENCE®

To better address the conflicts between duties of pre-trial Discovery and European Data Privacy Laws, the Working Group 6 of The Sedona Conference® has drafted the 2011 Public Comment Version of its International Principles on Discovery, Disclosure and Data Protection (the International Principles). This document contains six principles that attempt to facilitate the relationship between US discovery obligations and the EU Data Protection Directive.

The International Principles are not legally binding. Nevertheless, TSC®, as a non-partisan law and policy think tank, is considered to provide influential guidelines and best practices that are increasingly cited in leading judicial decisions.

3.3.1. THE SIX INTERNATIONAL PRINCIPLES

1. *With regard to data that is subject to preservation, disclosure, or discovery, courts and parties should demonstrate due respect to the data protection laws of any foreign sovereign and the interests of any person who is subject to or benefits from such laws.*

International comity compels "due respect" for the laws of other nations. By definition, however, international comity[60] is not without limits, *e.g.*, data protection laws may not be advanced for improper purposes or to delay discovery.

2. *Where full compliance with both data protection laws and preservation, disclosure, and discovery obligations presents a conflict, a party's conduct should be judged by a court or data protection authority under a standard of good faith and reasonableness.*

The parties' actions should accordingly be governed by standards of good faith and reasonableness. In *Aérospatiale*, the US Supreme Court, referred to the (Third) Restatement of Foreign Relations Law Section 442(1)(a) and ruled that US courts must be proportionate when balancing domestic discovery obligations with the interests of a foreign sovereign. The Principle urges that these considerations should be applied when deciding on conflicting legal obligations.

3. *Preservation, disclosure, and discovery of protected data should be limited in scope to that which is relevant and necessary to support any party's claim or defence in order to minimize conflicts of law and impact on the data subject.*

The controller, the requesting party and the court are obliged to protect the rights of data subjects and to minimize conflicts with Data Protection Laws. Both goals can be achieved through co-operation, stipulation or court order.

The Working Group 6 proposed the following actions to put this principle into practice:

- Limiting the scope of the request
- Being specific during discovery
- Using a schedule to enable chronological phased discovery, *i.e.*, parties agree on deadlines and the sequence of the discovery, starting the process with less problematic data and moving on to the more problematic data. The main purpose of the scheduling is to give sufficient time to "legitimize" the processing and transfer of data
- Minimizing the production of protected data, which includes filtering data, substituting alternative data and limiting the format of production
- Substituting data through alternative sources
- Limiting the format of production.

4. *Where a conflict exists between data protection laws and preservation, disclosure, or discovery obligations, a stipulation or court order should be employed to protect protected data and minimize the conflict.*

This Principle urges the parties to enter into stipulations or agreements that create legal obligations and assign duties to the requesting party to protect the data in a manner consistent with the applicable data protection laws. If the parties cannot reach an agreement, the responding party should seek a protective order that may be submitted to the court unilaterally.

5. *A data controller subject to preservation, disclosure, or discovery obligations should be prepared to demonstrate that data protection obligations have been addressed and that appropriate data protection safeguards have been instituted.*

[60] Restatement (Third) of Foreign Relations Law: "Comity, in the legal sense, is neither a matter of absolute obligation, on the one hand, nor of mere courtesy and good will, upon the other. But it is the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, having due regard both to international duty and convenience and to the rights of its own citizens or of other persons who are under the protection of its laws"

This Principle urges data controllers to generate sufficient evidentiary material, such as documentation, protocols, *etc.*, to provide proof as to the processes undertaken and show that reasonable efforts have been made to provide adequate safeguards for protected data processed or transferred for the purposes of US litigation.

6. *Data controllers should retain protected data only as long as necessary to satisfy legal or business needs. While a legal action is pending or remains reasonably anticipated, data controllers should preserve relevant information, including relevant protected data, with appropriate data safeguards.*

This Principle provides guidance on data retention policies and the specific scope and duration of the obligation to preserve data that is relevant to US litigation. It also recognizes that the potential conflict between discovery obligations and data protection laws is lessened through reasonable and systematic record management rules, provided they are applied uniformly and not in a fashion to avoid a litigant's common law duty to preserve relevant information once the litigant is on notice of actual or reasonably anticipated litigation.

3.4. SANCTIONS FOR VIOLATIONS OF PRIVACY LAWS

Violations of privacy laws may represent an administrative offence.[61] In Germany, administrative offences can be punishable by a fine of up to €50,000 and, in exceptional cases, up to €300,000. In the United Kingdom, fines can exceed €580,000. Fines might be levied if transfers or uses of personal data to a third party in the United States are not processed or used for the purpose for which they were transferred, or if the data subjects were not properly informed about the data processing. According to Section 45 of the German Data Protection Act, anyone willfully committing such an offence with the intention of harming another person may be liable to imprisonment for up to two years or to a fine.

[61] Section 45 of the German Data Protection Act (BDSG)

4. Final Conclusions

The transfer of personal data to an opposing party in the United States as part of discovery proceedings is particularly sensitive from the point of view of data protection. The United States is considered to be a third country that lacks an adequate level of protection. Furthermore, the receiving party in the United States is typically not subject to European law and may not, therefore, have the data protection concerns of the European party. The discovery process can, however, be influenced and shaped by the parties to the proceedings.

For both parties, discovery is associated with discomfort so the willingness of the parties to find solutions of the type advocated the six Principles of TSC® is therefore very likely. The parties are free to apply technical and organizational measures to protect personal data and to compromise on sufficient guarantees and safeguards for data subjects. Such compromises could be identified by the parties during procedural meetings such as the "meet and confer conference". This flexibility allows, in most cases, the avoidance of legal conflicts and, if an agreement cannot be reached, the possibility remains that US courts can issue protective orders. With adequate advance planning and understanding of these aspects, risks can be controlled and mitigated accordingly.

Glossary

Controller	The controller is the natural or legal person, public authority, agency or any other body that alone, or jointly with others, determines the purposes and means of the processing of personal data. Where the purposes and means of processing are determined by national or EU laws or regulations, the controller or the specific criteria for his or her nomination may be designated by national or EU law. (Article 2(d) Data Protection Directive)
Data subject	An identified or identifiable person to whom the personal data relate. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity. (Article 2(a) Data Protection Directive)
Third country	Any country other than the EU and EEA Member States
Personal data	Any information relating to an identified or identifiable natural person (a data subject)
Data processor	The natural or legal person, public authority, agency or any other body that processes personal data on behalf of the controller. (Article 2(e) Data Protection Directive)
Processing of personal data	Any operation or set of operations that is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. (Article 2 (b) Data Protection Directive)
Sensitive data	Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; data concerning health or sex life; and data relating to offences, criminal convictions or security measures. (Article 8 Data Protection Directive)

For more information, please contact your regular McDermott lawyer, or:

Alexander Harguth, PhD: +1 49 89 12712 161 aharguth@mwe.com

Alexander Harguth is a partner based in the Firm's Munich office. He has been representing German and international companies for more than 17 years. His practice is focused on patent litigation, including advising clients on complex infringement proceedings in German patent infringement courts and related parallel nullity and opposition proceedings in technical areas such as chemicals, pharmaceuticals, medical devises, electronics, telecommunications and mechanical engineering. Alexander is admitted to practice before all District Courts and Courts of Appeal in Germany and is also admitted as a French Attorney-at-Law in Paris.

Geoffrey Vance: +1 312 984 7593 gvance@mwe.com

Geoffrey Vance is a partner based in the Firm's Chicago office. Formerly the partner-in-charge of the Trial Practice Group in Chicago, Geoffrey is now the leader of the McDermott Discovery practice group. He regularly assists clients in creating practical, creative and cost-effective solutions for businesses to store and manage electronically stored information, both before and during litigation. Geoffrey is an active member of The Sedona Conference's® Working Group on Electronic Document Retention and Production and is also a working member of the Electronic Discovery Reference Model group charged with developing guidelines and standards for clients and providers of software and services related to electronic discovery.

For more information about McDermott Will & Emery visit www.mwe.com