Christian Zeunert / David Rosenthal

E-discovery and data protection: Challenges and solutions for multinational companies

Zitiervorschlag: Christian Zeunert / David Rosenthal, E-discovery and data protection: Challenges and Solutions für multinational companies, in: Jusletter IT 6 Juni 2012

Jusletter IT – Die Zeitschrift für IT und Recht
ISSN 1664-848X

www.weblaw.ch

E-discovery and data protection: Challenges and solutions for multinational companies

Authors: Christian Zeunert, David Rosenthal
Category: Scientific Articles
Field of law: Data security, E-Discovery
Region: Switzerland, USA

Multinational companies doing business in the US are likely to become involved in legal proceedings and, thus, likely to face e-discovery. Due to the global manner in which business as well as IT-related processes are set up in such companies, a legal proceeding in the US regularly has an international dimension. However, cross-border e-discovery raises both a number of organisational issues as well as legal questions, particularly with regard to data protection. This article discusses these issues, practical solutions and best practices. David Rosenthal focuses on legal aspects, Christian Zeunert on organisational issues.

Zitiervorschlag: Christian Zeunert, David Rosenthal, E-discovery and data protection: Challenges and solutions for multinational companies, in: Jusletter IT 6. Juni 2012

Table of Contents

1 Introduction

[RZ 1]

Much can be said about the challenges e-discovery pose to multinational companies. The same applies to data protection. Each of these concepts grew out of a specific legal culture, and neither may be ignored by multinationals, who by their very nature are exposed to both. The problem uniquely facing such firms is that e-discovery and data protection seem to place conflicting demands on them: a US-style pre-trial discovery requires companies to rigorously disclose any documents deemed even remotely relevant to the case, before the actual trial begins. At the same

time, European Union (EU)-style data protection statutes place severe restrictions on such disclosure and are guided entirely by the principle of data reduction and data economy, especially where data is to be shared with third parties.

[RZ 2]

And yet multinationals are expected to live by both concepts and must ultimately find a way to reconcile these contradictions. They must because they are firmly caught between both legal cultures when drawn into legal disputes in the US (and other jurisdictions with a similar legal system) while subject to a host of data protection laws in Europe and elsewhere with regard to the documents and information they process. All these companies generally seek to do is what any well-run organisation would want, namely, to comply with all requirements under applicable law as best they can.

[RZ 3]

While complex, universal legal compliance is achievable in many cases, it seems not to be so in the area of interest here: at the crossroads of e-discovery and data protection, many multinational firms inevitably find themselves pursuing conflicting objectives and, at first glance, having to choose between two evils – either severely restricting an e-discovery (or refusing to conduct one) or else acting in breach of data protection legislation. This certainly seemed to be the conundrum when amendments to the US Federal Rules of Civil Procedure in 2006 clarified the conditions under which e-discovery rules extend also to electronically stored information (ESI). In hindsight these changes opened the floodgates further on the practice of collecting and disclosing data processed in firms, and provided the cornerstone for e-discovery as we know it today.

[RZ 4]

The reactions of lawyers, courts and companies west of the Atlantic contrasted sharply from those of their peers to the east once it dawned on them just how extensive an e-discovery can be under US procedural law, and how valuable the information thus gained – internal e-mails included – can be to the matter in dispute.

[RZ 5]

When preparing for legal proceedings in the US, lawyers began listing documents and data of every conceivable category in their discovery requests[1] even if these requests were worded so broadly that the documents to be discovered were bound to include numerous files whose relevance to the case at hand was nil or highly unlikely at best. This in turn led counsel of either side to strongly advise their clients in pre-trial meetings to preserve any documents and data even remotely relevant to a case. They further cautioned them against risking any exposure whatsoever to court sanctions for destruction of evidence. (In some US jurisdictions, courts are known to hand down such sanctions whether or not the offending party acted in bad faith[2].) The clients were also advised to err on the safe side and disclose too much rather than too little.

[RZ 6]

Meanwhile, data protection officials and specialists across Europe raised a warning finger. They pointed out that anyone merely sending data to the US and discovering it there was in breach of the law – especially if the data sent turned out to be irrelevant. It was obvious to them that any e-discovery produces vast amounts of personal data and – worse – irrelevant personal data, and that

full disclosure of such data is hardly consistent with the principle of proportionality in handling personal data.

[RZ 7]

The battle lines were quickly drawn. The one camp received backing from the magistrates in the US who ordered documents to be discovered irrespective of European data protection laws, the other from EU data protection bodies such as the Article 29 Data Protection Working Party[3]. This body issued a working paper[4] with demands so far-reaching as to render e-discovering entirely impractical if they were heeded to the letter. Both EU data protection law and US civil procedural law provide scope for weighing up competing interests and so allow for more narrow interpretations of their own underlying principles. At the same time, neither law accords equal status to the interests of the other camp, if indeed these were even a consideration when the laws were drafted.

[RZ 8]

Until recently, both camps were equally guilty of favouring such ignorance and antagonism over dialogue. Companies caught in the middle without the option of avoiding the conflict would find themselves having to do more than just lobby all stakeholders to come to the table and forge a doable compromise. Above all, they needed to educate the stakeholders enough for these to realise that anything less than a compromise would not do. And education is exactly what happened in recent years, in a process driven mainly by multinational companies exposed to both legal cultures. Facing a US legal proceeding, such companies began contracting European outside counsel in addition to the standard American legal representatives, grooming e-discovery project owners within their organisation, and reaching out to their peers.

[RZ 9]

These efforts are gradually bearing fruit as more and more US judges, counsel and government agencies become aware of the many restrictive provisions of EU data protection legislation which apply to companies and which multinationals cannot ignore at will. Data protection officials for their part have recognised that a firm planning to do business in the US market will have to get familiar with all applicable law of the US legal system sooner or later, just as US companies operating in the EU are subject to the European system. And they do see that some concessions on data protection (including on the right of individuals to have their data erased or rectified), while inevitable, can reasonably be granted without stripping data protection legislation of its essence[5].

[RZ 10]

This text discusses the above conflicting objectives – and how to reconcile them – from the perspective of multinationals. After describing the legal and organisational challenges faced by firms with cross-border operations, the authors explore the legal and organisational approaches these companies take to discovery (and e-discovery in particular) today as they pursue viable compromises at acceptable risks.

2 Starting point for multinational companies

2.1 Overview

[RZ 11]

The challenges arising from cross border e-discovery in a data protection context are partly legal and partly organisational in nature.

[RZ 12]

At the legal level, other than the clashes between the divergent philosophies underpinning the US and continental European legal cultures, there are five other major challenges to consider, namely, the extremely vast scope of data protection laws, in geographical reach as in subject matter; the principles of legitimacy, transparency and proportionality; safeguards to protect the rights of data subjects; and the special regulations governing cross-border disclosure of personal data to the US and other countries that – from a European perspective – lack an «adequate» level of protection for personal data.

[RZ 13]

At the organisational level the core challenges beyond case-specific and company-wide interests boil down to four: ensuring the timely involvement of e-discovery specialists with an entrepreneurial mindset, gaining understanding and cooperation for the special requirements from the individuals who are parties to the dispute, managing the extra time needed to meet those requirements of European data protection legislation, and the practical application to the case at hand given that many tools have yet to be developed or adjusted for such purpose.

[RZ 14]

At the legal level in particular, these challenges arise not only in the event of an e-discovery but also in the context of discovery procedures in general; in other words, even where disclosure involves non-electronic documents. That said, given the volume of data stored electronically in most companies nowadays, and the availability of many printed documents also in electronic formats, which are easier to process than hardcopies, most issues that arise in day-to-day work relate to e-discovery. Experience shows that e-discovery generates not only far more material but also significantly more material that is pulled but irrelevant to the inquiry or whose potential disclosure was not anticipated by the data subjects involved, which is yet another concern from a data protection perspective.

2.2 Legal challenges

2.2.1 Conflicting legal cultures

[RZ 15]

As mentioned above, the particular legal challenges a multinational company faces in complying with an e-discovery in the Anglo-Saxon tradition lie mainly in being caught between competing legal systems without any way to avoid the conflict, given operational and business constraints. As described, the only option available to the firm is to pursue a compromise whose likely outcome will be viable for its business.

[RZ 16]

These legal conflicts flow from the divergent traditions in UK-US law versus Continental European law. Under US procedural law, for example, all parties to a legal proceeding assume as a matter of course that each of them will first preserve and gather any data and materials in its own area that could be deemed potentially relevant; then deliver this data and materials to its US legal counsel for review; and finally make the data and materials available to all parties to the legal proceeding – including the opposing party, in other words – for evidentiary purposes. This usually happens during the pre-trial discovery. Although a party could be forced to produce such data and materials, this is normally not necessary. Controversal discussions may typically arise over the scope, timetable and nature of a discovery or of the discovery requests of either party[6] which

under the US Rules of Civil Procedure the parties should discuss in the *meet and confer*talks early on[7]. One consequence of this tradition of producing any documents deemed even remotely relevant (even if damaging) is for instance that many companies now limit the period of (pre-trial) document preservation[8] to a minimum: just a few months sometimes, and rarely longer than 18 months. The situation is similar in other common-law countries.

[RZ 17]

The legal tradition in Continental Europe could not be more different. There, rather than being bound by the principle of total transparency, each party is free to produce the evidence it deems necessary to support its position. Unlike in the US, parties are not required to include damaging documents in a discovery. Often, an opposing party or third party can be compelled to a limited discovery only, if at all, and only under narrowly defined conditions. Accordingly, companies operating in Continental European jurisdictions tend to retain their records considerably longer than do their counterparts in Anglo-Saxon countries. In fact, the former are often required by law to store their business records – including e-mails – for many years. It is not uncommon for companies to keep these records for five or ten years. Many keep them for longer, in order to be at an advantage should it come to a dispute: they know that – in Continental European courtrooms at least – the odds are minimal that the opposing party will have to be given access to such records.

[RZ 18]

These differences between the Anglo-Saxon and Continental European legal cultures are enough to create legal issues for multinationals as soon as these plan to integrate their IT and their organisations across borders and continents. How long should a company keep records, for example? The answer to this question will vary region by region or even country by country, although more and more companies, citing costs, are switching to centralised electronic records management systems and processes.

[RZ 19]

Yet while country-specific records-management rules *can* be met in each country by technological and organisational means, a multinational's business activities will routinely cross borders. And because some of these activities are bound to end in legal disputes sooner or later, the multinational company inevitably will be caught between the frontlines of the two competing legal cultures mentioned above.

[RZ 20]

Scenarios of this sort are becoming more common as more and more internal units are being interlinked, and tasks shared, across borders. Increasingly, businesses are managed not only from a single location but also across legal systems. The dictates of efficiency also drive the centralisation of certain group functions and so give rise to organisational structures where in a dispute information that is deemed potentially relevant to the case is not only scattered all over the globe but is also managed by various affiliates and third-party providers.

[RZ 21]

For example, if the US subsidiary of a European multinational is the defendant party to a US civil action, the pre-trial discovery associated with that action may by implication extend to records kept at the firm's headquarters in Europe. For the purposes of a firm's discovery duty under US procedural law, it is sufficient for the records in question to be accessible to the parties to the legal

proceeding. This means that the US subsidiary can be made to discover parent-company records if the parent has made them available to the subsidiary via remote network access. Where the parent company itself is the defendant party – as is frequently the case – it can be ordered directly to disclose all records before it is even clear that there is in fact a case for (co-)indicting the European-based parent.

[RZ 22]

A US court may order a person based in its jurisdiction to disclose a broad spectrum of data this person actually possesses, has in custody or controls, regardless of their physical location[9]. In such cases, US law does not require compliance with applicable international accords such as the Hague Convention on Taking of Evidence Abroad in Civil or Commercial Matters – not even where the records in question are kept in foreign territory. The judge may subpoena a party to the proceedings to discover its records if it has refused to do so before. This subpoena will stand even if the actual order to disclose foreign-based records is allowed only once the particulars of the case have been considered[10]. Continental European law does counter these tendencies in US law, which does not necessarily make life easier for a multinational firm. For instance, the laws of various countries, including Switzerland and France, specifically protect the state sovereignty against acts of foreign courts and other public authorities. Under these statutes, the circumvention of the judicial or administrative assistance by privately gathering evidence in these territories may constitute a punishable offence[11]. Often referred to as *blocking statutes*, theses laws sometimes prohibit entities from disclosing even their own records in proceedings abroad to which they are party. So where a company is subpoenaed also by the foreign judge to disclose its own records, it will have to choose between two evils – unless it has made timely provisions to steer clear of such a dilemma.

[RZ 23]

Indeed, most multinationals can generally avoid this dilemma. In Switzerland for example even conservative scholars interpret the relevant legislation – Art. 271 of the Swiss Penal Code (SPC) – to mean that an entity is only prohibited from disclosing own records in proceedings to which it is party if said entity is being ordered (subpoenaed) or forced to do so[12]. In other words, an entity will not be liable to Swiss prosecution under Art. 271 if disclosing own records as part of a voluntary pre-trial discovery. If however a company refuses a reasonable disclosure request from the opposing party because it is gambling on averting a discovery of damaging records, then that company may simply find itself in deeper trouble later on. This is because a subsequent court-ordered subpoena to discover the records would eliminate the option of discovering them outside the legal assistance procedure even if the company were prepared to do so then – the consequences of which would be worse still. As this scenario illustrates, companies are well advised to look into the potential implications of non-cooperation – under non-US as well as US law – early on. For expediency, some discovery managers will weigh the relative threat of sanctions. In Switzerland for example a discovery manager will find that contravening data protection statutes in a pre-trial discovery tends to invite far less serious sanctions (if any) than violating Art. 271 SPC as a result of a discovery by court order[13].

[RZ 24]

Once a company is in this dilemma, international mutual legal assistance can help resolve only some of the issues involved even if the US judge is willing to provide it. For example, not all

countries in Europe are signatories to the aforementioned Hague Convention on the Taking of Evidence Abroad, and some who are have expressed reservations about disclosing records for the purposes of a discovery[14].

[RZ 25]

Other signatories to the Hague Convention do allow the gathering evidence on a broad scope through mutual legal assistance procedures and they even exclude the applicability of the normal data protection legislation, at least in cases where all parties agree[15]. Here too, the US perspective requires certain compromises, such as on the time window allowable for the taking of evidence[16] or the scope and the standard to be set for its prior specification, which in some cases may exceed the standard set by US law. Likewise, contractual or legal secrecy duties may, if they prohibit discovery in proceedings involving third parties or if they prohibit the export of materials[17], put multinationals in a bind, especially if compliance with these duties is secured by criminal law. Such secrecy duties have partially been designed with a specific view to safeguard trade secrets from disclosure abroad[18]. In such cases, discovering records in US proceedings may render the employees responsible liable to prosecution – at least if no further safeguards[19] were taken – even if their employer was ordered by a US court to disclose the records.

[RZ 26]

In the day-to-day operations of multinationals, however, data protection is the main source of conflict between discovery duties in US civil proceedings and Continental European law. The challenges it involves are discussed below. Data protection in its current form has been with us for many years, but more recently public perception of its merits, and companies' legal compliance, have been growing, while sanctions handed down for breaches have become tougher in various countries[20].

2.2.2 The five legal challenges of data protection

[RZ 27]

In matters of discovery, data protection creates particular challenges for multinationals. From the companies' perspective, these challenges can be summarised in five points as follows:

2.2.2.1 First challenge: scope

[RZ 28]

The first challenge arising from the conflicting demands of discovery on the one hand and data protection on the other is the broad ambit of data protection legislation, with regard to the subject matter as well as geographically.

[RZ 29]

First, many data protection laws are extensive in terms of their *geographical scope*: any e-discovery project involving Europe, even marginally, may be subject to the national data protection laws of any EU member state in which data is to be collected or processed for an e-discovery. In the EU for example national data protection laws usually apply if the*data controller*, i.e. in simple terms the person or unit responsible for data processing (in an e-discovery, typically the employer whose employees supply the data and whose servers compile the data for the discovery), is based in the country in which the data were gathered or – if the person or unit responsible is not based in the EU – the data are processed in the EU (as in a case where e-discovery data from non-EU jurisdictions are pooled on servers in the EU prior to further processing).

[RZ 30]

Complying with data protection provisions can be a major effort even for a company operating in just one single legal system. Multinationals by contrast must be familiar and compliant with the data protection laws of any country in which data need to be collected for e-discovery purposes or in which these data are processed further, and potentially even in the countries of discovery subjects whose national laws assert wider jurisdiction than is customary in Europe.

[RZ 31]

Swiss data protection law is a case in point: it may be applied even if a person whose data are subject to a discovery («data subject») is a permanent resident of Switzerland but his or her data are collected and processed abroad only[21]. It follows from this that any data gathering which presumably will include the personal data of Swiss residents or Swiss nationals among others will be subject also to Swiss federal data protection statutes, even if all data gathering and processing in connection with an e-discovery occurred or will occur strictly outside of Switzerland. Because Swiss federal data protection statutes extend to legal persons as well – as shown below – it is bound to apply in some form or other to multinationals with significant connections to Switzerland. From a company's *legal compliance* perspective this means that the firm must be capable either of classifying its data by applicable law or of adopting the strictest of all potentially applicable law (even if applicable only with regard to a subset of the data). In practice multinationals tend to choose the latter option, because data classified by jurisdiction is often unavailable and differentiated compliance therefore is impractical.

[RZ 32]

From a subject matter perspective as well the reach of European-style data protection statutes is extensive. These tend to turn on the concept of «personal data», which refers to all information relating to an identified or identifiable individual[22]. In some legal systems this concept is defined more narrowly[23]. In others, it is defined more loosely to include the personal data of legal persons as well as that of natural persons[24]. This may affect multinationals disproportionately, for example in situations where – as described above – centralised data processing may lead to the same data being subject to the data protection laws of several legal systems at once, thus forcing a multinational to choose between two options: either to adhere to the strictest law applicable (which in the present context would require protecting the data of legal persons as well) or to risk contravening certain national data protection laws (by focusing in-house data protection measures on the data of natural persons). Experience shows that many multinationals opt for the latter and leave it to their local subsidiaries to take more extensive measures if and as needed.

[RZ 33]

In any case, the scope of data protection is extensive, due to the ubiquity of personal data. Although the debate on data protection in e-discovery revolves mainly around the e-mails of employees of companies that are subject to an e-discovery, data protection is far more extensive in scope. It also protects the data of any other person who is identified, or who is identifiable by use of further information. In other words, data protection extends equally to any references in a company's e-mails, text documents or databases to other individuals such as clients, business partners or competitors (or their corporate bodies or other employees, to the extent that a legal system protects only the data of natural persons and does not exclude those of employees) whether or not their protection requirements are lower.

[RZ 34]

In e-discovery projects in practice, this is a recurrent source of misunderstandings and false expectations on both sides of the Atlantic:

- For one thing, *personal data* as a concept is often more narrowly defined in US law than it is in practice. (Another term, *personally identifiable information*, has become popular in the US and, while defined inconsistently, is sometimes used to mean the same as personal data[25]). It is not uncommon, for instance, for a US court to upon request extend a protective order for safeguarding business secrets in pre-trial discovery data to provide the same protections also to all personal data. Parties will often only later on realize that this means that more or less any and all e-mails, documents and data discovered must be kept confidential. Hardly a document in a pre-trial discovery will ever be entirely free of personal data as defined by European data protection law, except where such a document has been painstakingly anonymised, a practice routinely followed only for sensitive data and even then only selectively. Another common source of misconceptions is confusions of the concepts of *personal data* and *private data*. Typically, the former refers to personal data as defined above and as such includes data that, while relating to individuals, are of a business nature nonetheless. Private data by contrast are strictly private personal data; this concept refers to personal data not of a business nature.
- For another, data protection specialists in Europe and trial lawyers in the US frequently think in different categories in their respective areas. European data protection specialists want to regulate the processing of certain types of information as such, wherever and however such processing may occur. US trial lawyers meanwhile focus on the container of information, that is to say the document or dataset within which certain information is contained. Distinguishing as they do between content and carrier or form can be quite relevant, such as when data protection safeguards are being agreed or court-ordered. It is not sufficient to protect only documents as such; the protection must extend beyond to also include any verbal communications and the transfer of information contained in these document to other documents, even if these other documents are not part of the discovery, such as a legal brief or a written court verdict.

2.2.2.2 Second challenge: legitimate purpose and transparency

[RZ 35]

The next challenge in making e-discovery projects data protection compliant is the principle of legitimate purpose and transparency[26]. Simply put, these principles require that individuals affected are informed of the purposes for which their personal data is to be collected and processed[27]. Any subsequent change of the purpose for which such personal data is processed is a violation of these principles and is permissible only with suitable justification[28].

[RZ 36]

In the context of a discovery this means that all individuals subject to the process – not only the company's own employees – must have a clear understanding of the permitted uses of their personal data at the time when it is collected by their employer. They must understand that their data may be used in civil litigation in the US should their employer or one of its affiliates become party to such litigation. Express notification can reasonably be provided where its recipients are limited to a company's own workforce (for example, through general information in internal policies and specific information in actual cases before their data is being preserved). However, prior

notification is normally not reasonably possible where it would require reaching other data subjects (such as employees of clients, business partners and other third parties mentioned in the e-mails). In practice, these individuals are normally not provided with an express notification, partly on the grounds that anyone who communicates with a company these days as a rule must anticipate that the company may become involved in legal disputes abroad as well and that its records may be subject to discovery at that stage. In the event, the company's obligation will be to ensure that none of the personal data used in the discovery is used improperly. In other words, the company must ensure that the opposing party, the court and any other individuals involved use this data strictly for the purposes of the legal proceeding and, in particular, that none of the data is released to the public.

[RZ 37]

Ensuring this may not be a major challenge in the case of a company that operates only on a national level. In a multinational, however, adhering to the rule of legitimate purpose and transparency is a major challenge. This is because the use of someone's personal data is no longer necessarily limited to the purposes of the company with which the data subject is in direct contact and which is known to him or her. Whether through networking among and task sharing among a multinational's affiliates or by sheer coincidence, these data can easily find their way into legal disputes of other affiliates and, with that, into other legal systems. For example, if an employee of a US multinational's German affiliate is involved in a US project and that project then leads to a civil proceeding, e-mail correspondence between this employee and his German clients may also find its way into the pre-trial discovery in the US.

[RZ 38]

Here too it is of course perfectly reasonable to argue that employees should expect to be exposed to such data transfers as much as third parties are. And that they should expect so even more if dealing with a company affiliated with a multinational. Under most data protection laws, however, groups of companies have not been accorded a special status: the transfer of personal data among affiliated companies generally qualifies as a data transfer among third parties, which requires prior notification of the individuals whose personal data is to be transferred. No prior notification is required where an affiliate is merely acting on behalf of the group company that procured the data in the first place, but this will rarely be the case in the types of situations that are relevant to discovery. In addition, many legal systems accord special protection to the personal data of a company's own employees, thereby complicating any exchange of employee data between this company and others – even if such exchange were intended simply as assistance by one affiliate to another in the latter's court trial.

2.2.2.3 Third challenge: proportionality

[RZ 39]

The third challenge of data protection law as it relates to e-discovery lies in the principle of proportionality which this law applies to any processing of personal data. Simply put, the principle calls for personal data to be processed only as is necessary and suitable for the use intended, and only as is reasonably acceptable for the data subjects[29]. In an e-discovery context this means that generally data should be disclosed only inasmuch as its disclosure is essential to the case at hand.

[RZ 40]

European data protection specialists – the aforementioned Article 29 Working Party first and foremost – have inferred from this principle of proportionality the requirement that any information to be produced in a pre-trial discovery in US proceedings must first be filtered accordingly. In its 2009 working paper, which discusses the tension between the requirements of EU data protection law versus those of US pre-trial discovery, the Working Party also comments on adherence to the principle of proportionality[30]. To give effect to this principle, it says, either irrelevant personal data must be removed or the existing information must be anonymised or pseudonymised. This means stripping the data of any references to individuals, for example by redacting real names or replacing them with a pseudonym[31]. The Working Party's rationale for this is that in and of itself, disclosure of irrelevant personal data as part of a discovery is a breach of data protection principles because by definition, processing these data is not relevant to the legal dispute. So if the identity of a given data subject (such as the sender or recipient of an e-mail message) is not relevant to the litigation at hand, then that identity must not be revealed, according to the Working Party. In this body's view the culling of irrelevant data must happen in the country of origin (before the relevant data is transferred to a third country such as the US) and is best done by a «trustworthy third party» with knowledge of, but no stake in, the litigation[32].

[RZ 41]

The European data protection community is gradually coming round to recognising such requirements as being unreasonable, unrealistic and unviable for businesses. And with some good will, less stringent requirements can be derived from EU data protection law. (One approach that easily satisfies the proportionality rule is discussed in Chapter 3.3.2 below.) The key concern, however, which is to avoid any unnecessary processing of personal data, remains valid. And yet poor acceptance of this concern is not the issue; the latter exists in US procedural law as well. Rather, the challenge in real life lies in the divergent views about the extent to which disclosing records is in fact essential to the dispute: what is truly relevant, and what can reasonably be demanded of a party? Although known to the US Federal Rules of Civil Procedure even before these were amended in 2006, the proportionality rule was rarely invoked in the past. It started drawing more attention only very recently, most likely in the wake of excessive e-discovery demands. Disclosing records irrelevant to the case itself may become necessary all the same – for example, if their non-disclosure in an e-discovery were to prevent a proper verification of how the relevance and compliance of a culling process was determined by a party. Or if at the time of discovery there are not enough resources, information or time available to cull all irrelevant records in the first place.

[RZ 42]

Ultimately, what is relevant and what is not again is a matter of definition. What *is* relevant to the discovery is reflected above all in the parties' discovery requests and should be an outcome of the *meet and confer* talks or, if these fail to produce an agreement, from a corresponding court order. It is up to each party to find a way to select from its total pool of documents and data, wherever possible, only those records for discovery that belong to the subset of relevant records as defined in a previous step. Any selection errors tend to be accepted only where they favour more extensive disclosure. As a rule, then, a company need not disclose all those e-mails that meet certain formal, external criteria (such as from-to dates, recipient, sender, and/or keywords). These criteria are applied merely to begin narrowing down the selection. The company will however subject the remaining records to a semiautomatic culling process, disclosing those hits that meet

certain search criteria and that in a manual review by the company's own legal counsel were not clearly recognised as irrelevant (or as exempt from disclosure for other reasons). So selecting the right keywords and the right search strategy and refining them («keyword refinement») is key in determining the subset of information for discovery. What remains by and large is what may be deemed relevant and in practice will be disclosed.

[RZ 43]

Of course, this subset too will shrink over time, because invariably many questions fall by the wayside or become less relevant as a legal proceeding wears on. In the end only a few questions will remain and it will be for the court to decide which e-mails (and other evidence) it intends to consider in ruling on the case, as only these will matter in its view. This is not to suggest that it was improper or gratuitous to disclose all the other e-mails at earlier stages in the proceeding. Often, establishing what exactly the trial will be about – let alone what will be relevant – is mostly guesswork. (Unlike in the Continental European legal system, a suit brought in an Anglo-Saxon jurisdiction need not be very specific.) This and the fact that the pre-trial discovery comes before the trial means that the challenge ultimately lies in culling the data in such a way that a minimum of proportionality is ensured despite the uncertainty.

[RZ 44]

One point to note is that the data processing to be considered as per the rules discussed here may begin before a suit is filed: under the US Rules of Civil Procedure the parties to a legal proceeding are obliged to preserve any likely relevant information from the moment the legal proceeding must reasonably be anticipated. Accordingly, the threat of legal action an in-house counsel receives by way of a phone call may be sufficient to cause a company to issue a legal hold (a written instruction not to delete or amend any and all records that may be relevant to such proceeding) and to use appropriate tools at this stage already to ensure their preservation and availability for use in the event of legal action. There is no general obligation to collect and separately store all data. However, if at risk of being changed, deleted or lost otherwise, the data must be preserved already at the time of the legal hold. One way of doing so is by transferring the data to a dedicated data storage system. As mentioned above, carelessness in this area may result in serious consequences for the relevant party in any subsequent litigation.

[RZ 45]

All these processes are relevant in terms of data protection law in that the personal data involved are being processed for an additional purpose (i.e. the potential use in litigation), for one thing, and may be stored for longer than is customary under the circumstances (i.e. longer than is typically necessary from the company's perspective), for another. Once records are being preserved for additional purposes or for longer than normally, this immediately raises questions about compliance with the aforementioned data protection principles of legitimate purpose, transparency and proportionality in the processing of personal data.

[RZ 46]

Adhering to these rules presents a challenge not only for multinational companies. But it can affect a multinational disproportionately in cases where a discovery extends to not just one but numerous subsidiaries abroad and where data therefore must be collected in the most diverse legal systems and consolidated. For reasons of uniformity of processing as much as for efficiency and cost effectiveness, it will be unrealistic in most such cases to undertake the culling in each country

separately before all data is consolidated (see the standard procedure as set out under Chapter 3.3.2 below).

[RZ 47]

It should at this juncture be said, though, that the proportionality rule entails not only restrictions for the company concerned[33]. Data protection regulations do not call for every conceivable action that might be in the interest of protecting the information of data subjects. The regulations merely insist on safeguards that are reasonable. The less sensitive the data and the less adverse the data subjects' interests in their data being processed are, the less stringent are the data protection requirements for the person or entity processing their data. This rule of thumb is often forgotten.

2.2.2.4 Fourth challenge: rights of data subjects

[RZ 48]

The fourth challenge concerns the guarantee of the rights of individuals who are data subjects. These rights entitle data subjects to access their personal data, to have such data rectified or erased and to object to their data being processed[34]. In general these rights also apply to any personal data disclosed in a discovery. Here again data protection presents a challenge not only to multinationals. Specifically, their challenge lies in that the court and the opposing party to whom the relevant personal data are to be disclosed tend not to recognise the right of individuals to access their personal data, to have it amended or deleted and to object to its processing.

2.2.2.5 Fifth challenge: cross-border disclosure

[RZ 49]

The fifth challenge of data protection in a discovery context consists of restrictions on transborder disclosure of personal data. These restrictions vary somewhat country by country, even within the EU, although the basic regulatory concept is the same in every European nation, including Switzerland. According to this concept, personal data (with some exceptions) may be exported only to third countries that provide for an adequate data protection, whether by law or guaranteed through some other measure[35]. In the context of a discovery in a US civil proceeding, these export regulations are often considered to be of very high relevance, but they should not be overestimated. Ultimately their objective is to ensure that personal data is processed only within a tight framework even outside Europe and in countries where data protection is not the law. In Europe this framework is guaranteed by law, and transferring data collected for e-discovery purposes, between EU member states and to third countries the former recognise as safe, including Switzerland, is not a real issue. (Depending on the country, national law may impose certain additional restrictions also on exports of personal data to a «whitelisted» third country outside the EU/EEA[36], which is why even in such cases consideration should be given to the national data protection law requirements in the country of export.)

[RZ 50]

Yet special safeguards are called for whenever data collected is to be transferred to the US, whether to the company's own attorneys or, later, to the opposing party for discovery purposes. As the US has no data protection legislation in place that according to the prevailing opinion qualifies as adequate by European standards, European companies need to either ensure data protection by some other means or seek exemption from this requirement by providing sufficient justification.

[RZ 51]

The most popular approach used in transferring data internationally today is to conclude a transborder data transfer agreement. In some civil proceedings this type of agreement may be an option for a European company's communications with its US attorneys but hardly for those with the opposing party and certainly not for those with the court. This is the case in countries where in practice only the model clauses approved by the European Commission may be used. In countries where local data protection law gives data exporters more leeway in designing a measure for ensuring data protection abroad[37], there may be case-specific solutions for satisfying data protection export restrictions such as protective orders containing provisions that (also) address data protection.

[RZ 52]

Another option would be to obtain permission from the data subjects. In practice this approach tends to fail as not all of these individuals can usually be reached prior to disclosure; any permission they might grant only after disclosure may be null and void for legal reasons. Besides, their permission has legal force only if granted voluntarily, which, according to the legal view prevailing in some European countries, is not usually the case with employees who are not members of senior management.

[RZ 53]

As a consequence, under European data protection law only two other means of legally exporting personal data are available if a flexible solution of the above sort is not an option. Either the US recipient of the data identified for discovery has self-certified compliance with the Safe Harbor Privacy Framework[38] on the use of these data, thereby submitting itself to the key principles of data protection as practiced in Europe, or an exemption is invoked under European data protection law which allows personal data to be transferred if such is required for asserting, exercising or defending legal claims[39]. The scope of such exemption does tend to vary according to interpretation in different European countries. Occasionally it is claimed that an exemption may be invoked only in cases of international judicial assistance, which would make it seem rather redundant. More often, however, the exemption can be relied upon in the case of an e-discovery, provided certain measures are implemented to ensure that the data disclosed in the foreign proceeding is not used for other purposes, among other things[40].

[RZ 54]

Against this background, the challenge for multinationals in particular lies in using the different rules in different European countries to the best of their advantage and steering clear of unfavourable export arrangements. For instance, if data from various European subsidiaries need to be collected for a US legal proceeding, the most obvious solution may be to export the data from each subsidiary directly to the US. This solution, however, is also the most complex: Although all European countries in general provide for a similar level of data protection, the formalities for exporting personal data to «unsafe» countries significantly vary among the various European jurisdictions. This can increase compliance costs, complicate matters and cause delays. Hence, it may be a better solution to first pool all e-discovery data collected in Europe in one European country, as the movement of data within Europe is normally possible without or only few or no restrictions and formalities. Once the data has been pooled in such a European country, the onward

transfer of the data to the US is much easier as only one data protection regime (the one of the country from where the data is exported) has to be complied with in this regard.

2.3 Organisational challenges

2.3.1 Case-specific and groupwide interests

[RZ 55]

More often than not, the organizational challenges particular to a multinational group involved in a legal case with international e-discovery essentially boil down to this: the employees in charge of managing the case may tend to see it from a narrowly case-specific, local-company perspective first, and will therefore start adopting an integral, group-wide view only much later, which sometimes may be too late.

[RZ 56]

The consequences of this kind of approach are compounded by the failure of these individuals to fully appreciate the international dimensions of the case and, as a result, to recognize the case as being an international case at all. And yet, in a multinational company, issues that appear to be local at first glance may swiftly grow to international proportions, in all kinds of ways. Plainly, this makes handling such an issue much more complex. The international aspect even of seemingly local activities will be consistently recognized at the European entities of a multinational but tends to be ignored all too often at its US entities.

[RZ 57]

Hence defining standard global guidelines and processes should be a group-level task for multinationals also in the area of e-discovery and should not be left solely to their US entities. At many multinationals, this is bound to be a challenge as US e-discovery is often perceived as a matter concerning the US only. Only gradually is it being recognized as the global issue it should be to any multinational. The sometimes exorbitant sanctions handed down in the US for flaws in a legal hold and disclosure as part of the pre-trial discovery may long have been one reason why the relevant processes have focused mainly on complying with US procedural law. In more and more cases, however, noncompliance with other countries' legislation on the subject – European law in particular – in connection with conducting e-discovery may result not only in significant reputational damage but also in fines (such as are handed down for data-protection issues) or criminal prosecution of individual managers (for breach of so called blocking statutes that exist in some countries and may prohibit the collection or export of evidence for a foreign proceeding, for example).

2.3.2 The four organisational challenges of an international e-discovery

[RZ 58]

The international nature of e-discovery presents multinational companies with additional challenges at the organizational level. From the firms' perspective, these challenges can be summarized in four points as follows:

2.3.2.1 The first challenge: getting e-discovery experts on board early on

[RZ 59]

How can someone assigned to handle a legal case in the US recognize early on that cross-border e-discovery might be involved and assess what consequences this will imply for the case at hand?

[RZ 60]

Ultimately, this question arises in any litigation that a multinational company finds itself drawn into in the US. Answering it is likely, at first, to baffle most individuals tasked with handling such cases[41]. There are two reasons for this. One, in many multinationals each such case is handled by different individuals, who then lack prior experience. Two, a consistent pattern found in many multinationals is that case handlers are neither e-discovery specialists nor familiar with specific IT (never mind the systems used in their own companies) nor with data protection legislation and other relevant legal terms of reference prevailing outside the US. Their expertise will be of a different sort: either they are in-house counsel with more or less experience in litigation and some knowledge of applicable US law, or they are particularly connected to the matter at the heart of the case and have been made the case handlers for that reason.

[RZ 61]

Actual experience shows that such case handlers may not know the correct questions, let alone the legal, organizational and technical requirements involved in securing and obtaining evidence outside the US, such as data protection standards or the content of relevant blocking statutes and their implications. Nor are they likely to have the time and the resources to acquire such knowledge in any detail. Negotiating this obstacle is the first major challenge facing organizations, which must comply with these standards no matter the level of awareness or knowledge of their case handler.

[RZ 62]

Absolutely key to preparing for any anticipated US litigation is for the case handler to contact one or more e-discovery experts (in-house if available, else outside the company) at the earliest stage. Experience shows that for multinationals and their subsidiaries, the external US trial lawyers usually mandated to represent them in a specific case are not the ideal partners to contact in such cases:

[RZ 63]

For one thing, many US trial lawyers – even if they are not known to admit as much – remain largely inexperienced in running e-discovery projects, and have had even less exposure to e-discovery processes extending beyond US borders. It is true that more and more big US law firms have been in-sourcing e-discovery partners or counsels, some of whom have gained extensive experience also in cross-border e-discovery projects[42]. In practice, however, cost considerations all too often mean that such outside expertise is not sought in every case, or not from the outset, at any rate[43]. For another, outside counsel typically are unfamiliar with the specific situation at the company with regard to the areas relevant to e-discovery.

[RZ 64]

This is because in multinational companies, which tend to contract outside counsel in large numbers, a lack of continuity normally hampers these relationships at the individual level as much as at the law-firm level: The partners entrusted with the case are bound to change even if the law firms themselves do not, and the associates change more often still, even though they ought to know the company-specific circumstances best, given that they tend to be ones doing the actual work in a discovery.

[RZ 65]

It is more reliable and efficient and also more cost-effective to create an internal e-discovery organization or, at a minimum, to establish a stable relationship with a specific e-discovery service provider or a law firm or consultancy specialized in e-discovery that can advise not only in forensic matters but also independently of a specific case or merely case-by-case, while other law firms actually represent the company in court. This organization or consultancy need not be based in the US at all.

[RZ 66]

What is usually necessary however is that the organization or service provider is brought aboard from the moment new litigation is anticipated – in other words, from the very beginning. Under the US Federal Rules of Civil Procedure, this is also when the company's duty to preserve any documents and data that may be relevant to the litigation starts, and the company must employ the organizational and technological resources necessary in ensuring that no potential evidence can be destroyed from that moment on.

[RZ 67]

Ultimately, the only means available to this end is initiating a standardized global (and centrally controlled) legal-hold process, as there seem to be no other way to ensure that data protection requirements and other international aspects are duly considered in US litigation, which, by its very nature, most times starts out with an US focus. Using a standardized process of this sort also ensures that the specialists will have sufficient time to run a standard cross border e-discovery analysis[44] before the actual discovery has even begun and to change tracks if and as necessary.

[RZ 68]

Most times it is already too late to do so once the retained counsel has met and conferred with the counterparty on how to conduct the discovery[45], because the basic parameters for the discovery must be in place and complied with by that stage. To this day, unfortunately, there are many outside counsel in the US who meet and confer with the counterparty before having met with their client to discuss the particular legal and organizational challenges involved in a cross-border type of e-discovery – the variety commonly facing multinationals – and to define realistic parameters. As a consequence, these challenges are not taken into account in good time. If the European special requirements are then asserted at a time when the rules for conducting the pre-trial discovery have already been agreed with the counterparty, and if the schedule is as tight as it usually is, then calls for such requirements to be met usually fall on deaf ears.

[RZ 69]

Where no standard processes have been put in place to take such requirements into account and so cannot be carried out in a timely manner, one of two outcomes is highly likely, neither of them desirable. One, that any risk assessment that might be adequate from a company or case perspective may fall by the wayside, at the expense of compliance with data protection laws and other non-US legal requirements. Second, that the company may find itself unable to honor the protocols established in the *meet and confer* process.

2.3.2.2 The second challenge: educating, and working together

[RZ 70]

In Europe as well as the US, even legal professionals are often only starting to grasp the legal requirements of data protection in Europe and the actual impact these will have on a discovery process. There is a need for action at all levels: the company must educate its own employees, the outside counsel retained and those of its counterparty, as well as the US judges, on how these requirements may determine the type and scope of a discovery, its timetable and the need for further arrangements, and solicit these stakeholders' cooperation as needed to meet said requirements.

[RZ 71]

Sadly, experience suggests that the vast majority of US judges will at best be mildly sympathetic to European concerns about data protection, as they too race against the clock to work through vastly diverse cases. The subject of e-discovery in and of itself will be uncharted territory to the average US magistrate, who may face enormous challenges when expected to rule on such matters given the massive impact such rulings may have on the costs and the burden of proof required in court. That a serious knowledge gap exists in this area has now been recognized as a fact in the US[46] and more and more training programs are coming on stream there to address it. Along with this, US judges tend to focus on their «home market» first, with barely any interest or resources to spare for whatever special requirements may come from abroad regarding how an e-discovery should be conducted.

[RZ 72]

All the more important, then, for multinationals – whose exposure to such special requirements is largely inevitable – to be proactive about finding a solution to the challenges they face in this area. In practice, this invariably means working through the*meet and confer* to address and resolve the matter of European data protection requirements and the additional challenges, legal and otherwise, involved in a cross-border e-discovery.

[RZ 73]

Sadly, experience shows that the US Federal Rule of Civil Procedure 26 (f) dated back to December 2006 is not yet standard practice with all US attorneys. Rather than listening to the other side's concerns and working to find mutually acceptable solutions, too many are motivated by “tactical” considerations instead, resorting to excessive demands or refusing outright to cooperate[47]. For the clients of either side, this means incurring unnecessary and significant costs at best or, in a worst-case scenario, facing strategic disadvantages in the legal proceeding and a discovery by court order, and a subpoena if they challenge the order. In Switzerland, for example, specific legal hurdles (Art. 271 of the Swiss Penal Code) exist which may severely limit a company's options with regard to handling the documents it has stored there, and which may put the company at a serious disadvantage in the legal proceeding. Any multinational company whose plan is to avoid these scenarios therefore needs to have discussed, in advance, its own situation in terms of conducting a group-wide e-discovery case also under the technological, organizational and legal conditions prevailing outside the US. The company needs to have done this so it can educate its external US lawyers and other stakeholders on its particular circumstances and the standards it must comply with – at any time, without delay and in a documented form – and articulate the corresponding guidelines for action in an actual legal dispute. All of this preparation needs to be completed before

the *meet and confer* begins – indeed, before an actual case even arises. Otherwise, there will not be sufficient time for the thorough kind of evaluation required, as experience has shown. This in turn means first raising awareness within the relevant units in-house to educate them on the planned course of action, given the substantial costs routinely involved even in laying such groundwork – costs that can rarely be charged directly to any specific litigation.

[RZ 74]

Moreover, the course of action as devised should be discussed with the people who will be involved in the discovery. For example, rather than retaining just any law firms to represent them in court, multinationals tend to seek longer-term relationships with an outside counsel panel of selected, preferred firms. This type of arrangement lends itself to pre-discussing the special challenges of a cross-border e-discovery and the measures planned with the relevant key contacts at the panel law firms – in general terms and during routine client-attorney meetings – and agreeing the standard course of action to be taken, but also building the necessary relationships between the company's own case handlers and any e-discovery specialists before any litigation arises. Such preliminary measures in themselves may dramatically improve a multinational's scope for action when it faces actual litigation, and may reduce the burden and costs of any subsequent e-discovery.

2.3.2.3 The third challenge: time-consuming additional measures

[RZ 75]

If homework is not done the steps required to comply with local legal requirements, while more time intensive in some jurisdictions than in others, nearly always end up delaying the discovery process at least partly. Assessing the legal ramifications alone may take several weeks, unless it is done in advance. The company should keep this fact in mind when meeting and conferring with the counterparty on the discovery schedule to adhere to.

[RZ 76]

In practice, one approach that has proven useful has the parties agree on phased discovery, starting with the – typically straightforward – US data if any. This avoids delaying the start of the discovery process while buying sufficient time for the multinational to obtain and disclose the relevant data from locations outside the US and especially from Europe[48].

2.3.2.4 The fourth challenge: compliance in practice

[RZ 77]

Yet another practical challenge facing multinational companies is to be meticulous enough in complying with the e-discovery requirements under US law[49]. It should come as no surprise then that these requirements are forever being likened to a minefield where at least one fateful misstep per case is a certain prospect for any company. And where e-discovery takes on a cross-border dimension, with a raft of additional requirements as described above, implementing the rules becomes even more challenging.

[RZ 78]

One of the difficulties routinely facing multinationals is that the processes[50] developed by the industry bodies and experts – and the tools (software solutions) to implement them – often cater only to the US domestic market. Sadly, the European call for «data privacy by design» has been largely ignored by e-discovery software makers and is only gradually being addressed by their solutions.

[RZ 79]

This means that the task of initiating and implementing compliance with these requirements is left to the multinationals themselves. While the corresponding procedures are relatively easy to define and adapt on paper, their actual implementation is time intensive and can be costly.

[RZ 80]

For instance, when embarking on legal-hold and discovery processes, companies routinely find themselves having to modify the parameters software makers set for access rights to internal databases and systems. They need to modify them to allow for the required number of different roles and locations of the users involved in these processes, and to effectively restrict these users' access to only those database subsets and systems components that are essential to their ability to perform their legal-hold and/or discovery work. This includes sorting the data by their geographical origin, precisely a job that many software solutions are not yet designed to do. Some for example do not provide for «country of origin» as a meta-data category by which documents might be classified, lumping all data together instead. Where such classification is unavailable, geographical scoping – in other words, creating subsets of documents by origin – requires using a workaround. In other words, a company will be forced either to apply the strictest data-protection standards to all data indiscriminately or else accept its non-compliance with those standards, whereas scoping would enable it to apply them narrowly to relevant data.

[RZ 81]

Even the sophisticated database filtering and culling tools available today are hardly easy to use if they are to deliver the desired results. Handling them requires the requisite specialist training and experience, yet few if any attorneys appointed to handle a case will have the necessary methodological and technical know-how. Many e-discovery service providers do offer the latest technologies in the field, along with the manpower trained to use it, but more often than not will be contracted by the company's outside counsel and not by the company directly, and as such take instructions only from the former.

[RZ 82]

In practice, this means that minimizing costs is often treated as less important than it likely is to many companies and clients: the less care and focus is given at the first stage to iterative culling of the data collected for a discovery, the greater the data volumes for subsequent manual review by counsel – and the higher the costs for the client's account. Meticulous keyword refinement and testing is frequently skipped, because the expertise required is not available in-house or helpful know-how that often is available is left untapped, or because the typical US trial lawyer does not mind if the discovery includes more irrelevant documents than is necessary, or for all of the above reasons. Done thoroughly, however, keyword refinement in practice is a highly proven cost-cutting tool and, from a data-protection perspective, an effective culling mechanism for discovery-relevant data. Hence more and more multinational companies are faced with the challenge of in-sourcing these processes and building the necessary expertise in-house.

3 Workable solutions for multinational companies

3.1 Introductory remarks

[RZ 83]

While handling the organizational challenges may be a matter of sheer effort and goodwill, it seems illusory (at first glance at least) to conduct an e-discovery in Europe expecting to fully satisfy US law and European data protection legislation as well as other applicable legal requirements.

[RZ 84]

At a closer look, it becomes clear that by approaching the problem with some flexibility and an open mind set, it is in fact possible to find solutions that are workable and acceptable to all parties involved. Such solutions have also become the subject of discussions being held at the relevant international bodies, including the Sedona Conference[51], and is increasingly gaining favor among those advocating full disclosure during the process as well as among data protection officials. Proposed solutions of this kind – some of which are described below – are premised on three conditions, however:

[RZ 85]

First, the party ordered to carry out a discovery inquiry in Europe must be willing in principle to disclose all relevant documents to the extent permitted under applicable law in each jurisdiction. While required or taken for granted under US procedural law, such willingness to cooperate is not a given from a European perspective. This is because the principle of total transparency as applied to a discovery runs entirely counter to the continental European legal tradition and in particular because the costs of an e-discovery, including the subsequent review of the results, are potentially staggering (In the US alone an e-discovery conducted for a major lawsuit may cost a party up to several million USD[52].). Occasionally, parties to a legal action in a European country undermine the spirit of data protection law by abusing its provisions and other legislation to avert disclosure through seemingly insurmountable obstacles. In recent years, however, experience has shown that in most cases the majority of European companies will agree (albeit grudgingly) to cooperate if involved in a civil suit brought in an Anglo-Saxon jurisdiction as a result of their business activities. The same is even truer of multinationals with permanent branches in the US. There is hardly a European group or group headquarters not prepared to assist its US subsidiary in a local dispute if reasonably able to do so. Nor should the influence of legal advisors be underestimated: whenever a European company finds itself involved in some legal action in the US, it will invariably retain a legal representative for cases heard by a federal court. (In international arbitration, disclosure tends to be handled with much more restraint, although there too a trend to more expansive interpretation can be seen, driven predominantly by lawyers steeped in the US tradition.) Refusing disclosure is virtually unthinkable for US lawyers, however. Motivated by tactical considerations as much as by their native legal tradition and understanding of their role as servants of the law, they will disclose any even only loosely relevant – but not privileged – documents reviewed as part of a discovery, against their client's will if necessary, also to cover themselves.

[RZ 86]

Second, European firms should prepare for such an event and take the necessary precautions if they are at a non-negligible risk of being drawn into a US civil suit and facing discovery proceedings as a result. There is no other way to ensure that in the event of such legal action they will proceed systematically, appropriately and with some degree of efficiency: a pre-trial discovery

– the most common trigger of an e-discovery – is no long-term project. Rather, it typically must be organized within weeks and completed within months, bearing in mind that the initial planning – the legal hold in particular – must be under way across all group companies before a suit is filed or at a minimum must be feasible at any time without delay and in an orderly and well-documented fashion. Rarely ever is there time to investigate the legal requirements in any detail or to rehearse in such a case. True, data protection laws and other legislation in Europe provide some scope for making an e-discovery more difficult to carry out or for limiting its reach. Also, US courts have demonstrated noticeably more understanding and consideration when confronted with such obstacles in recent years. At the same time, they can see from their experience of real-life cases and the ongoing debate in specialist bodies and the literature that many of these obstacles can in fact be minimized if the defendant company demonstrates some goodwill. And, rightly or wrongly, the courts implicitly expect such goodwill from the defendant company. European firms will do well therefore to demonstrate similar goodwill and to make it plain that any legal hurdles to a discovery are not down to any failure on their part to do their homework. Not all US courts hold companies to the same high standards when it comes to their ability to conduct a state-of-the-art e-discovery. But where a company falls short because it failed to prepare properly, it risks being held liable for gross negligence in certain jurisdictions and facing the kind of sanctions handed down for such offences, regardless of whether the company acted in bad faith. This applies to multinational groups in particular, whom any US judge will deem sufficiently resourced and knowledgeable to conduct a comprehensive e-discovery efficiently, at home and abroad. In other words, more and more judges in the US these days expect multinationals to be aware of the e-discovery scenarios they may face down the road, and to prepare accordingly.

[RZ 87]

Third, independent of concrete measures, it is important for all parties to a legal action to familiarize themselves in some way or other with the legal tradition and mindset of their opponent in the cross border setting. While not given in national disputes, such awareness is indispensable in a transatlantic context. A crucial role in educating his or her own camp may come to the in-house counsel or case handler. This role involves ensuring that representing outside counsel will pull in the same direction and coordinate their actions early on. For example, this may mean coordinating with each other before the scope, milestones and procedures of an e-discovery are agreed with the opponent in the*meet and confer* discussions in a given case. In their external relations as well, companies are well advised to be proactive about educating the court and their opponents on the requirements under European data protection law where a discovery may (and, in the case of multinationals, nearly always will) involve collecting data and documents also in Europe and other non-US jurisdictions. Even today, the duty to ensure such awareness in US civil suits rests squarely on the shoulders of the company facing cross border implications, despite the growing appreciation in the US in recent years of the challenges posed by European data protection laws.

3.2 Understanding the company's own particular situation

[RZ 88]

Companies store different kinds of data depending on their own particular business purpose. In addition, each and every firm is organized differently. Then there is the degree of globalization which even in multinationals will vary in terms of their business processes, cross-border cooperation among their group companies and the centralization of their IT infrastructure.

[RZ 89]

Thus, any firm that intends to assess internally the likely scope and consequences of a cross-border e-discovery in specific US litigation needs to first understand its own situation in terms of the relevant parameters. The firm needs to grasp how its own processes work in actual fact and not just on paper, what sort of data is involved and where it flows and where, how and how long it is stored.

[RZ 90]

As shown time and again above, it is indispensable for a company to understand its own particular situation before going into *meet and confer* discussions with the counterparty at the start of a US legal action, so it is properly prepared. To do so it is not enough for the company to be able to satisfy the counterparty's standard request for a catalogue of relevant data systems and their accessibility. No less crucially, the company must establish in advance the potential territorial scope of an e-discovery and of the legal entities concerned, so it can point out any potential issues, legal or otherwise, in good time. And lastly, it must be able to gauge how sensitive the different categories of data actually are in terms of the various recognized legal requirements, as some data sources will always be more affected by such restrictions than others. Here, too, the company needs to have done its homework before it can react as timely and efficiently as needed when meeting and conferring with the counterparty and during the e-discovery itself.

[RZ 91]

Following below, this article will first highlight the special organizational and technological aspects of multinationals that have been shown to be particularly important in case-specific analyses of cross-border e-discoveries. Next, it will explain how such an analysis is performed, and then point out two further developments and tools which may help multinationals understand and handle their own particular situation better.

3.2.1 Organisational aspects particular to multinationals

[RZ 92]

First a company should know how and in which locations its value chain is managed. For many multinationals this process is spread across different countries. Accordingly, for example, research and development, production, marketing and distribution and central group functions may be run from different group companies in various countries but may all be affected by a specific legal case.

[RZ 93]

In many groups of companies even the execution of individual stages of their value chain is globalised, through virtual teams of employees scattered all over the globe, such as in a matrix organization, rather than through country-specific teams. These teams are based across a number of countries and affiliate companies.

[RZ 94]

The growing use of asynchronous communications media such as e-mail and other e-collaboration software (online forums and platforms in group-wide networks) further drives this trend. Concomitantly, e-discovery is becoming more complex and more global in scope.

[RZ 95]

Compounding these trends, more and more companies are off-shoring, near-shoring and classic outsourcing even their core processes. These organizational forms have a tremendous impact on all matters surrounding data access and monitoring. Hence they too should be known and documented for e-discovery activities and allow monitoring for this purpose.

3.2.2 IT aspects particular to multinationals

[RZ 96]

IT data management can vary as much in how it is set up from one multinational to another as can the organizational model. In practice, however, efficiency and cost considerations have led many companies to centralize their data storage continent by continent or to use cloud computing for less critical data, or to plan to do so. It used to be that each physical location would run local e-mail and file servers. These days, the trend is to consolidate such infrastructure at least by region and bundle it in one single or a few countries. And company database management trends are moving in the same direction.

[RZ 97]

Among other things, these trends have been gradually eroding any prior strict separation of US-based data from data stored in other countries, or else limiting such separation to only a few systems such as those of human resources departments or areas where applicable law prohibits exporting data even in the normal course of operations, if any.

[RZ 98]

By the same token, these trends mean that in performing their regular duties as well, US-based employees of multinationals are increasingly given access to data that originate and are stored outside the US. Here too, a company needs to know (and document) whom it intends to have access to what data, as the mere availability of remote data access to US employees may have direct e-discovery implications for the company. This is why data access – across affiliates and across borders, not just within each operation – should be properly managed and documented.

[RZ 99]

Next, the company should collect information on and document where it physically stores and performs backup routines of its electronic documents and data and where the associated applications are installed, so it can establish the geographical scope and the applicable legal framework of e-discovery purposes. Special attention should be paid to cases where certain data may be stored in several countries in parallel, which may simplify their discovery considerably in the event of different legal hurdles in the relevant jurisdictions. In some cases, such information may allow the company to take precautions as appropriate. For example, it may export copies of relevant data between affiliates should blocking statutes inadvertently prevent the disclosure of such data[53].

3.2.3 How to analyse a cross-border e-discovery in a multinational firm

[RZ 100]

Generally, a multinational will follow a multi-stage process when analyzing its own situation in terms of a cross-border e-discovery:

[RZ 101]

First, the firm needs to determine the scope of the data to be discovered. What type of documents will need to be produced in the context of the litigation at hand? Which of these data are stored in the firm, and where? What criteria could reasonably be applied in ring fencing such potentially relevant documents from other documents kept in the firm and ultimately in isolating the data identified for discovery? Several additional aspects which multinational companies need to consider in this regard have already been mentioned above. The answers to these questions should clarify which jurisdictions govern an e-discovery in a given legal case and which affiliate companies are affected. This in turn will depend on which jurisdictions and which affiliates the staff (directly and indirectly) affected live and work in, where the potentially relevant data are stored, and which affiliates are themselves a party to the case in question and which are only indirectly affected.

[RZ 102]

At this first stage the firm should also assess the nature of the potentially relevant data, establishing suitable categories. Are these sensitive personal data of employees, customers or other individuals? Are they data of former employees, in which case less stringent data protection provisions may apply? Will disclosure affect executive board members or other employees entrusted with company secrets? Will it affect data of third parties who by agreement or by law are assured special confidentiality or special data-protection safeguards?

[RZ 103]

At a second stage the multinational must find out where the expected US court trial will be held and according to what rules. Even within the US the rules, standards and practices that apply to e-discoveries will vary. Depending on the circumstances, the plaintiff may elect to bring a particular case in a federal district court or a state court, while the defendant party has certain leeway of its own to have a case transferred to a court it prefers.

[RZ 104]

At a third and last stage the multinational will need to establish which legal frameworks it must comply with when conducting a discovery outside the US, given the documents subject to discovery and the applicable provisions of US procedural law. Examples include EU data protection legislation where documents from the firm's European branches are concerned, or other legal norms such as the aforementioned blocking statutes. At the same stage, the company should analyze its options for meeting these requirements (such as agreements entered into for this purpose, or protective orders) and identify the person(s) within the company whose remit includes these ancillary measures and whether government agencies (such as national data protection agencies) must be involved.

3.2.3.1 Using internal e-discovery specialists

[RZ 105]

While outsourcing remains an ongoing trend in many areas, the very opposite is happening in terms of e-discovery in multinational companies: specialists and systems to handle these processes are being insourced across the board[54].

[RZ 106]

Costs are just one factor driving this. More and more companies of a certain size and global reach that have latent exposure to litigation risk in the US are building e-discovery know-how and

infrastructure in-house for further reasons: they will become more efficient and effective at working through the challenges involved in cross-border e-discovery projects, but also to mitigate risks in the international arena. This appears to be the motivation especially of a growing number of multinationals headquartered in Europe, whose targeted development of e-discovery specialists in-house is meant to move the process under better central control and, with that, ensure that it factors in the international dimensions to an e-discovery more regularly and, above all, from an early stage[55]. Accordingly, e-discovery units can be found in European as well as US-based multinationals, and in many of the former they are even run by Europeans.

[RZ 107]

Creating an internal e-discovery organisation and staffing it with the requisite specialists is an indispensable step also toward centralising and standardising group-wide the legal-hold and e-discovery processes as such[56], which conforms with the spirit of both European data protection statutes and, ultimately, US procedural law.

[RZ 108]

A company's internal e-discovery organisation also functions as an interface, in that it is able to coordinate the needs of the legal department, external counsel and IT and can be just as effective liaising with the records management, information security and internal data-protection units.

3.2.3.2 Using internal e-discovery systems

[RZ 109]

More and more multinationals are using workflow-based legal-hold systems[57]. This is because such systems not only help to make a legal hold more efficient and more defensible to perform, they also offer substantial advantages to companies as they prepare to disclose documents in a cross-border e-discovery. Depending on the used system it may permit to either directly preserve or collect data or at least send out preservation or collection plans centrally. Both ways will serve a critical requirement, that all actions performed per legal case are documented in a central place in line with applicable legal requirements. In addition, via such systems it is much easier to keep track of scope changes in respect of employees, data sources and timeframes involved. Keeping track of scope changes such as releasing custodians or data identified as not relevant during the discovery process is necessary from a data protection standpoint but pretty burdensome and less defensible if not handled via a system logging such steps appropiately.

[RZ 110]

Similarly, beyond preserving electronic correspondence for legal and business purposes, e-mail archiving systems – if offering the necessary functionalities – can be used for legal hold and e-discovery purposes as well. The IT and the legal department should work closely together to be able to define the full set of requirements for all relevant countries. Experience has shown[58] that the core strength of most of those systems is still to fulfill the IT storage requirements in case this is the vendor's core domain. The e-discovery solutions seemed to be «add-on solutions» which failed to provide European data protection requirements as purely developed with an US focus. For example, the ability to only grant access to e-discovery personal to the relevant proportion of the data e.g. scoped by country or at least custodian and time period at issue, has not been possible in the standard offering. The transparency requirement to grant employees access to «their» e-mails when it comes to the journaling of e-mails for preservation purposes has also not been foreseen. One solution to overcome such short comings may be to combine an archive with a search product.

Such combinations can be ideal both for preservation and early case management activities. Via the *preserve-in-place* option e-mails may be put on a legal hold on a case-by-case basis without any additional data transfer. In addition, it offers cost benefits while allowing for centralised and transparent monitoring of a legal hold's implementation. At the same time, such systems can be used to tag positive data by geographical relevance prior to data sharing and discovery.

[RZ 111]

If linked with sufficiently efficient and powerful search engines, such archiving systems can further assist in preparing for an e-discovery by enabling testing and refining of possible search terms ahead of the *meet and confer discussions*, without the data collected needing to be copied or exported to separate systems. This too saves time and money and ultimately helps strengthen data protection.

3.3 Accepting pragmatic compromises

3.3.1 Preliminary remarks

[RZ 112]

The second aspect to meeting the challenges facing multinationals in the context of e-discoveries involves pursuing workable compromises through measures that must be taken at the technological and the organizational levels.

[RZ 113]

What such compromises may look like in practice can be illustrated using the principle of proportionality as employed in data protection legislation. Following the recommendations of the Article 29 Data Protection Working Party in particular would mean having a third party review all discoverable data and – subject to the matter in dispute – anonymise and pseudonymise all discoverable data prior to discovery, in fact even prior to transmission to a another country. However, doing so would exceed both the time and the budget usually available and make further data analysis (including culling of irrelevant data) by the company's lawyers impossible.

[RZ 114]

By contrast, where a discovery run in the classic US tradition, the data collected as part of an e-discovery would be reviewed only for legally privileged content before disclosure. It would not involve any measures to protect the privacy of employees, for instance, as under US law any and all documents and data stored on an employer's systems are the exclusive property of that employer. There, the employer may dispose of these documents and data largely as it sees fit, even in court and even were such use results in their public disclosure.

[RZ 115]

On this point as well Europe follows a different philosophy: even at work, employees' privacy is protected to a certain degree, in that their employer may access their business e-mails but not, in principle, their personal correspondence – not even where employee regulations prohibit the use of personal e-mail at work. Where content is likely to be private, as in personal e-mail accounts, the employer's access is often subject to restrictions that may or may not actually be satisfiable depending on the interpretation of applicable data-protection legislation.

3.3.2 Standard procedure for conducting e-discovery in Europe

[RZ 116]

In and of itself, recognizing the conflict between European data protection laws on the one side and US full disclosure requirements on the other is of little use to multinationals. Conflict or no conflict, they routinely face having to carry out wide-ranging e-discoveries in their European operations as well. Inevitably, they need to strike some kind of compromise.

[RZ 117]

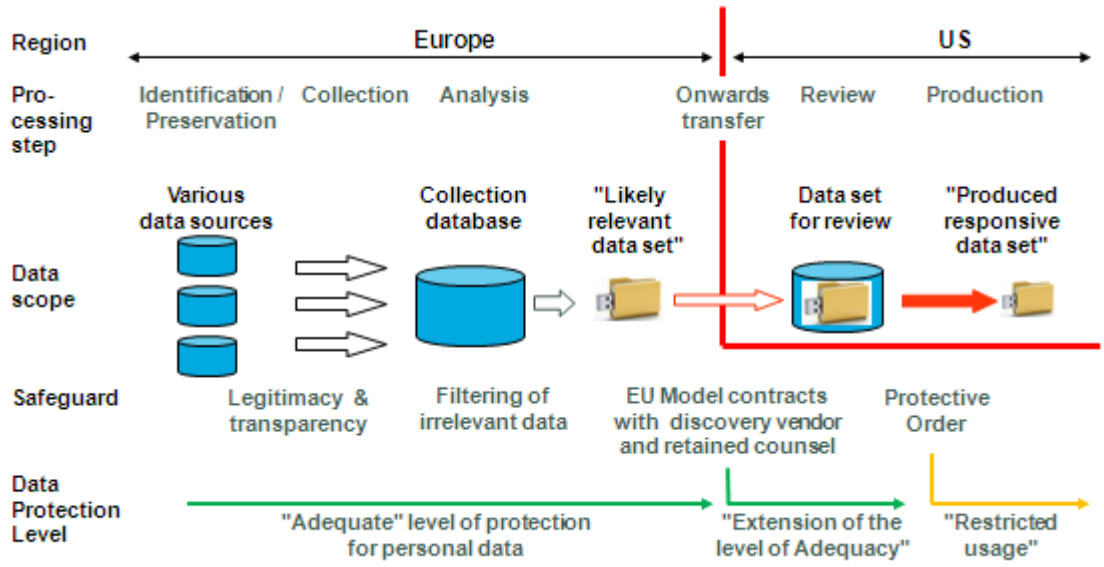
In response to these conditions a standard procedure evolved in recent years for e-discovery exercises in Europe, a procedure that has come to be widely used by multinationals in their efforts to comply with the requirements of both jurisdictions wherever possible[59]. Various versions of the procedure have been described in the literature and discussed in specialist bodies. The recently published «International Principles on Discovery, Disclosure & Data Protection» by The Sedona Conference Working Group 6 also contains a «Cross-Border Data Safeguarding Process + Transfer Protocol»[60], which reflects most of the thoughts below.

[RZ 118]

This procedure has proved to work surprisingly smoothly in practice. No incidents contravening data protection laws or significant interventions by data protection agencies have been reported. The procedure was even discussed with and welcomed by the Article 29 Data Protection Working Party even though it does not meet the standards set (or at least communicated originally[61]) by this body and merely represents a (useful) compromise. Quite likely, however, it is this very approach – preferring usability over perfection – that accounts for the procedure's success.

[RZ 119]

The diagram OVERVIEW OF CROSS-BORDER DISCOVERY PROTOCOLS below illustrates high level in which country which processing step on which data scope can be done by applying adequate safeguards achieving different data protection levels:



OVERVIEW OF CROSS-BORDER DISCOVERY PROTOCOLS

[RZ 120]

The procedure is flexible enough to be modified to suit numerous criteria and meet the requirements at hand. Broadly, it can be structured according to five stages as follows:

[RZ 121]

A first stage involves the targeted collection of forensically accurate copies of data pre-identified in every European subsidiary where relevant data may be stored, which is transparent to the affected employees. Following the written legal hold notice, the employees are given a questionnaire asking them to identify the data sources on which they have been storing any documents and information potentially relevant to the case at hand[62]. The questionnaire should prompt them to be as specific as possible and as expansive as necessary in answering the questions. This will ensure from the outset that no unreasonable amount of irrelevant data is collected later on. In addition, the employees should indicate whether in the identified targeted areas sensitive personal data or private data may be stored. In terms of the company systems familiar to them, the employees should be asked to be as precise as possible in identifying the area and type of personal data that is potentially relevant according to the scope instructions provided. For instance, they should indicate the folders they have been using for storing files on their local hard drives and network drives, if any, to avoid having entire computers or servers subject to the discovery, which tends to be the default procedure. Crucially, the employees should be given clear and detailed instructions on this point and their responses must be verified and followed up on, to avoid collecting data too narrow in scope and thus risking non-disclosure. If the legal-hold notice did not inform the employees of the need or obligation of their multinational to compile certain data as a precaution or for review in an actual dispute, this survey will close this gap and will do so before such data are collected. The reasons for collecting the data need to be explained by identifying clearly the legal proceeding for which the data will be needed to be preserved, processed, transferred and ultimately produced in the US or other venue at hand.

[RZ 122]

The legal-hold notice and the interviews are useful therefore to prevent not only potentially relevant documents being deleted or modified but also obviously irrelevant data being collected in the first place. Thus, the information as such and the process of interviewing employees also serves the interests of data protection while enabling the company to comply with its obligations under transparency provisions of data protection legislation. Given these circumstances, employees' express consent will no longer be required in the majority of cases, certainly not for data protection reasons. Frequently, this information is collected from employees also to address the issue of private content: employees are reminded either that in line with applicable company regulations, private content may not be stored at all or only in specific locations (such as dedicated directories on employees' local hard or network drive, the data of which are not collected for e-discovery purposes) or asked to remove their private data before the data is collected.

[RZ 123]

At a second stage the data collected in the European subsidiaries is often compiled in a central location in Europe using a proprietary database of the multinational or a so-called early case assessment database supplied by an e-discovery service provider; transferring the data within Europe is usually a straightforward matter in terms of data protection laws[63]. If the company in question already has an early case assessment suitable solution in place based on an archiving

solution (see Chapter 3.2.3.2 above) it may not be required to collect the data separately for the discovery purposes. To qualify, however, this solution would need to have been factory-designed to double as an early case assessment database for discovery purposes, with built-in security and data protection suitable features, filters and export interfaces. Inevitably, such archives will include large quantities of irrelevant information and possibly private data as well. Whether using a proprietary system or an archiving solution, the company must ensure that no data in scope can be deleted, modified or lost in non-compliance with the preservation obligation. (If using an archiving solution in parallel, the company must ensure in particular that the feature that automatically deletes data upon the end of their defined archiving period – frequently the default setting – is turned off for the affected data in scope, so that documents for relevant custodians are continued to be preserved for the duration of the legal hold). Access rights to the secured data should be restricted to a small group of individuals who have been trained for this purpose and are authorized on a case-by-case basis. For tracking and audit purposes, any operation performed on the database should be logged automatically as a single event and made retrievable through ad-hoc reports.

[RZ 124]

Where disclosure is initiated as part of a pre-trial discovery, **a third stage** involves culling the information gathered once or multiple times, semi-automatically, usually in the early case assessment database, to identify irrelevant documents and remove them physically or at least logically[64]. The data culling is performed manually, whereby e-discovery experts work with individuals familiar with the case to define culling and search parameters and to test and, where necessary, refine these down – for example, by entering key words, dates, file folders, document names, or sender and recipient names. This is done for the purpose of identifying and exporting all of those documents that are likely relevant excluding documents clearly irrelevant, to the case at hand, without having to view every single document. A tried-and-tested method for efficiently refining keywords is using identified terms by either excluding groups of false positives (separating them with the «NOT» operator) or by grouping keywords (operator «AND»)[65]. For obvious reasons, searches are often started with broad keywords, such as general descriptive terms, first or last names and case-specific abbreviations. Often, suppressing documents that otherwise will come up in search results even though they are in fact irrelevant – so-called false positives – requires working through numerous variations of different keyword and operator combinations, linked and non-linked, before an effective combination of search terms is found for extracting the documents identified for disclosure. This approach helps protect data privacy but also helps cut costs – the lower the data volume, the lower the costs of reviewing them. As a result, the process of culling is known and accepted in the US as well[66]. The parties, however, should agree this approach in writing during the *meet and confer*, including the culling criteria respectively search term refinement applied (hence the importance of running relevant searches, and preparing proposals based on the search results, ahead of such meeting). Specialists are being assisted by ever more powerful search and filter tools marketed these days by the makers of various e-discovery programs. However, the use cases and limits on how to use predictive coding software are discussed controversially following the *2012 Da Silva Moore* case opinion[67].

[RZ 125]

In the interest of data protection, initial culling should happen while the data are still in Europe, in the early case assessment database itself. The outcome will be a noticeably slimmer database of «likely relevant data». These data will not have been redacted or manually sorted, however. The only time a thorough manual review is usually conducted before the early case assessment database or the documents being saved to it are exported is when the mere act of exporting the data may result in criminal sanctions. As mentioned, this is sometimes the case in certain European countries with regard to specific types of business secrets, for example.

[RZ 126]

At a fourth stage the «likely relevant» data that has been collected and pre-culled is usually sent to the multinational's own lawyers in the US or is made available to these by remote access to the review system of an e-discovery provider in the US or in Europe[68]. Data protection specialists see the latter option – remote access – combined with keeping the data in Europe as interfering less with the privacy rights of any individuals affected. Providing remote access is preferable therefore to sending a full copy of the likely relevant data to the US. Yet, experience shows that with remote access to a database hosted in Europe, costs are up to 25% higher than if a US-based e-discovery provider is used. At the same time, these authors do not consider the European option, with remote access from the US, to be essential in case additional appropriate safeguards have to be in place, including for non data protection reasons such as protection against the risk of a forced disclosure by US authorities (which is usually less than the risk of an issue in a civil matter, but may be relevant in cases of governmental investigations). Also, granting remote access out of Europe to US attorneys located in the US may still be less costly than flying-in US lawyers to review documents on-site in Europe, which would be unreasonable to do purely for the sake of data protection (but may be warranted for other reasons such as statutory secrecy requirements that prohibit the export of certain documents). That said, we note that the costs of conducting reviews in Europe have meanwhile come down significantly; depending on the circumstances such as the languages at issue, the quality and efficiency of work may be higher when using local reviewers that are more familiar with the languages, the local environment and the local habits.

[RZ 127]

It is only at this fourth stage that there is a case-specific manual review of the data remaining after the culling. This review serves multiple purposes, one being to screen out any documents that are legally privileged and as such are exempted from disclosure or that are clearly irrelevant. Another purpose is to investigate the facts surrounding the case, in preparation of the proceedings to come. A third purpose may be to cull documents that are problematic from a data protection perspective, such as private or otherwise irrelevant files. That said, proper culling requires that the individuals tasked with reviewing the files have been instructed accordingly (and that all such instructions are documented, for subsequent tracking and auditing) and are able (i.e. have the knowledge and skills necessary) to put these instructions into practice. Where culling of private (that is, non-business) content is not permitted because it is contained in documents that are relevant otherwise, such non-business content may need to be redacted if necessary.

[RZ 128]

Whether it is sufficient to cull the private content remaining after the semi-automatic filtering process is a matter that will need to be determined case-by-case. From time to time, data

protection considerations may warrant a prior privacy review depending on the extent to which the company whose data are concerned informed its employees beforehand about how their data might be used. In other words, managers who fail to inform their direct reports beforehand may face having to spend extra time and energy reviewing data at a later stage.

[RZ 129]

In addition, it may be advisable to redact the names of employees included in content. This text argues however that even under European data protection law, it would be unreasonable to presume a general obligation to do so. Nor is redaction routinely applied in practice. Exceptions may be warranted in cases where an employee whose name is disclosed is likely to face serious negative consequences, such as personal claims or criminal prosecution by foreign authorities. In such cases, any employer duty of care toward its employees, if provided for under labor law, may be sufficient grounds for redacting the names of the employee in question, to the extent that such redaction is in line with national legislation and unless the name disclosed is that of a person who has already been exposed (as is usually the case with people in leadership positions, for instance).

[RZ 130]

However, such cases are clearly exceptional even in the normal course of business of multinationals. In all but a few commercial disputes, employees mentioned by name in an e-mail ultimately will not face any consequences themselves if their identity is disclosed as part of an e-discovery; at the most, they may be called upon to testify as a witness in the proceedings. If disclosing a person's identity will have no significant consequences for that person, and if redacting the person's name typically involves substantial effort and costs and in a discovery context is bound to prompt concerns over the right to redact, then redacting or not redacting the person's name becomes a matter of proportionality. An important point to remember is that even in data protection law the data privacy concerns of the person facing disclosure must ultimately be weighed against the interest in processing that person's data. In the same spirit, the aforementioned statement by the Article 29 Data Protection Working Party on the anonymisation of persons' names now tends to be interpreted as a recommendation rather than an obligation.

[RZ 131]

At a fifth and final stage the data manually reviewed and (where necessary) redacted during the fourth stage are disclosed by the US-based lawyers to the counterparty. In this process, the data leave the domain of the disclosing party. Still, safeguards can and should be put in place to ensure that the data is under some measure of protection even after it has been disclosed[69].

3.4 Documenting and regulating crossborder data transfers

3.4.1 Preliminary remark

[RZ 132]

In the above standard procedure, data is culled and transferred at different stages of an e-discovery, and its main benefit to European companies is that the two key principles of data protection, proportionality and transparency, can be satisfied (with some concessions) even in a US court-ordered e-discovery. Yet the same standard procedure is no help with other data-protection issues that arise in an e-discovery; addressing these involves further steps. Here too business practice has produced some pragmatic approaches that are suitable also for multinationals.

3.4.2 Crossborder disclosure

[RZ 133]

In the first instance, this concerns the challenge posed by data protection requirements for crossborder disclosure of personal data. Without disclosure across national borders, e-discovery is impossible in Europe. At the same time, the legal scope for such disclosure is limited, as discussed above[70]. This must be seen in terms of each of the various stages involved in the procedure. If the above e-discovery standard procedure is adopted, transborder disclosure of personal data begins with the consolidation of data within Europe. Typically, however, such consolidation is not subject to any restrictions under data protection law that add to costs or complexity, as the data transfers involved are within the EEA single market or else to a «safe» or «whitelisted» third country such as Switzerland.

[RZ 134]

There is a need for targeted action only when a company sets out to transfer its consolidated e-discovery data to the US, given that the US is not classified as a whitelisted third country from a European point of view. In most cases, an obvious way to still comply with applicable minimum data protection standards will be to enter into a formal agreement including the model clauses issued by the European Commission (EU model clauses). In practice this may well be the most popular method of safeguarding data that are going to be transferred to the US. Even so, experience shows that it may be worthwhile looking into other methods, and evaluating a range of possible scenarios even when using the EU model clauses. Multinationals in particular will do well to do so if they own subsidiaries in a number of countries including, in some cases, in the US. It will give them a broader range options with regard to possible exporters and importers of data: For example, it may be more straightforward and more efficient for a multinational first to transfer the data it has pooled from its European subsidiaries to a US parent or subsidiary affected and only then to make the data available to the attorneys in the US, rather than sending these attorneys the data in separate transfers from each subsidiary directly. This will be advisable for example where a suitable data transfer agreement with the US subsidiary is already in place or sufficient binding corporate rules exist within the multinational[71], or if the US subsidiary is Safe Harbour certified for the type of data in question[72]. In any case, the multinational will need to verify that applicable data protection regulations permit disclosing the data in a legal proceeding as well as transferring them to the company's own legal counsel. In real life this aspect is often ignored or left out, such as when the EU standard contractual clauses are used. The most popular standard clauses for data transfers between data controllers are the ones dated December 2004[73]. Pursuant to para. II(i) of these clauses, the transfer of personal data by data importers located outside the EEA, for example, is permitted only on certain conditions. Accordingly, such transfer may only be made to a safe third country (which excludes the US for companies without adequate Safe Harbour certification), or if the data importer becomes a signatory to the clauses (which an opposing party or the court in the US is unlikely to do), or if the data subjects have been given the opportunity to object once informed of the purposes of the transfer (which may be feasible in dealing with the company's own employees but with any other data subjects it certainly is not). Hence, if personal data is transferred to the US for discovery purposes, on the basis of these standard clauses, the discovery will invariably lead to a breach of contract. So if the data exporter is able to anticipate a breach he should not export the data, strictly speaking, even though he would be doing so having agreed the standard clauses. The EU standard clauses for transfers of personal data to processors,

of February 2010[74], are less restrictive on this point but may create different complications case-by-case because of certain additional requirements such transfers must meet in some EU member states[75]. There is far more leeway in cases where data transfers can be carried out with Safe Harbour certification. Certified companies are largely free, within the bounds of their data protection guidelines and the certification rules, to decide how to ensure adequate protection for any data they transfer onward. (Admittedly the onward transfer of personal data for discovery in a civil proceeding is rarely a consideration when firms define their data protection guidelines.) Meanwhile several notable US law firms and e-discovery service providers have become compliant with the Safe Harbour Privacy Framework through self-certification, which can be very helpful when data need to be transferred to these firms from an EEA country or Switzerland.

[RZ 135]

Consolidating European data for discovery purposes in one European country can streamline such a discovery significantly, as the rules of only one country have to be followed with regard to the envisaged data export into the unsafe country. The United Kingdom is one of the countries used for such purposes; Switzerland is another case in point: While Switzerland provides for the same level of data protection as all EU countries do, Swiss data protection law is much less formalistic as to the question *how* a particular level of data protection is achieved, as long as it *is* achieved. For instance, Switzerland does not prescribe any formal requirements, in law or in custom, as to how a contractual guarantee for ensuring an adequate level of data protection in an unsafe third country has to be worded, as long as the guarantee is adequate[76]. The EU standard clauses are recognised in Switzerland, as well. But a data exporter from Switzerland is free to make any alternative provisions (including ones rather shorter and simpler or occasionally more tailored to the case at hand) if these provisions serve to guarantee an adequate level of data protection on the data importer's side abroad[77]. Also, Switzerland's status as a safe third country[78] means that data collected in the EU for e-discovery purposes is usually easy to export to Switzerland. Once the data have been consolidated in Switzerland, their exportation is subject only to Swiss data protection law which, as discussed above, is less formalistic than the corresponding laws of certain other EU countries. This may be of key importance in the case of a legal proceeding where an opposing party will usually not be willing to enter into the EU standard clauses, but may be receptive for using alternative instruments such as protective orders adapted to provide for the necessary degree of data protection[79]. Such pragmatic solutions are possible under Swiss law. This is not to say that solutions like these necessarily come without challenges of their own. Switzerland does offer a far more flexible and, therefore, a more attractive regulatory environment than most of the EU when it comes to data protection. By the same token, the Swiss legal system is far more protective of its jurisdiction against the reach of foreign governments than are many of its peers. In and of itself, this is no hindrance to a company's voluntary participation in a pre-trial discovery. But the same disclosure is a punishable offence if made by US court order[80]. The above examples and discussions illustrate that the challenge involved in complying with data protection rules in a crossborder discovery is not whether compliance is possible but how best to go about it. In this regard, the very channels of communication often available to multinationals may prove an asset, as resolving the legal aspects of this challenge may require first routing the data streams accordingly.

3.4.3 Protecting the data post-discovery

[RZ 136]

As discussed above, a company's duty to protect personal data continues even after these data have been transferred to the US. A multinational should manage reasonably well to safeguard personal data while processing these data in-house or through the legal counsel retained but no longer, obviously, once the data have been disclosed to the opposing party (and subsequently to the court, if necessary).

[RZ 137]

That said, a standard procedure has emerged in recent years to address this issue as well. Although, depending on the circumstances, it may fall short of some or other data protection requirements, the procedure does address the key concern of data protection legislation in terms of a discovery, namely, preventing the use of personal data outside the courtroom or for other purposes.

[RZ 138]

The standard procedure entails the issuance of a protective order by the US court with jurisdiction on the case. As a rule, this order is drafted and negotiated by the parties jointly and is issued by the court, and covers any personal data disclosed in discovery. Protective orders are widely used in US civil proceedings but mainly to protect business secrets from disclosure by the opposing party and other persons involved in the legal proceeding, such as witnesses or experts. At the same time, a protective order ensures that the court will not make these records available to the public (as is customary with parties' submissions and documentary evidence filed in US civil proceedings[81]) but will keep them under seal instead.

[RZ 139]

As an alternative to a protective order, the parties may simply enter into a confidentiality agreement. The advantage of such an agreement is that it is faster to put in place and is out of court. On the downside, a confidentiality agreement is enforceable only on the parties thereto (but not on third parties, if any, to the legal proceeding) and even then only in terms of a breach of contract, not contempt of court. In practice, confidentiality agreements tend to be signed ahead of a discovery, such as during discovery negotiations or preliminary data sharing, whereas protective orders are used as a safeguard during the actual discovery process.

[RZ 140]

Because protective orders and confidentiality agreements are legal instruments known to and accepted by every US attorney and every US court, they have proved ideally suited in recent years to enforcing protection of personal data disclosed pre-trial or during a legal proceeding. To such end, all personal data (as defined under EU law) are governed by the same protections as are companies' trade secrets[82], on the one hand, while the recipients of such secrets on the other hand are not only bound by secrecy but are also prohibited from using the data for any purposes not directly related to the legal proceeding, to the extent that these recipients are not prohibited from doing so already. If the records are made available to third parties, it must be ensured that these parties too are subject to the restrictions of the protective order (or that a confidentiality agreement is in force which prohibits disclosure to third parties or limits such disclosure to certain defined conditions). As a rule, protective orders also stipulate that the records must be destroyed or returned after the legal proceeding has ended or after use.

[RZ 141]

There is one use for which a protective order is not necessarily appropriate, and that is enforcement of the data subject's right to access its personal data or to have such data rectified or erased. Often, US opposing parties will be unwilling to grant such rights bindingly to data subjects because to their minds, ultimately, these rights go too far. (Why for example should a party submit to the instruction of a person from the opposing camp if the instruction is that the party no longer use certain evidence or use it only in anonymised form?) At best they may agree to give favourable consideration to data subjects' assertions of such rights. Thus, if a data subject wishes to assert its rights to access its personal data or to have it rectified or erased or to object to it being processed, the data subject's only option will be to turn to the party that disclosed their personal data in the legal proceeding and to have that party ask the judge, in its own name, to instruct it accordingly or to give the data subject the necessary information (for example, about the volume of records disclosed that relate to the data subject).

[RZ 142]

However, situations like this are rather hypothetical. They hardly ever arise in practice and so do not usually conflict with a discovery of personal data in a US civil proceeding. Here again, any approach taken should emphasise practicality over perfection.

4 Summary

[RZ 143]

Pursuing e-discovery in multinational companies does raise legal and organisational issues, but with a pragmatic approach, these hurdles can be overcome in a reasonable manner.

[RZ 144]

On the legal side, the solution basically lies in adopting the principle of proportionality on both sides of the Atlantic: It is neither proportionate to require companies to disclose each and any piece of information regardless of whether such disclosure were to violate the personality rights of employees, customers and other third parties, nor is it proportionate to apply the rules of data protection in a manner that effectively prevent a company from participating in a pre-trial discovery. As experience shows, it is possible to find a compromise by applying procedures that limit any disclosure to what is really necessary for the purpose, but at the same time also require information to be removed or redacted prior to production only where this is really necessary to protect employees, customers or third parties. Fortunately, standard procedures have evolved on how to do so in multinational e-discovery exercises that involve Europe or other jurisdictions that have implemented stringent data protection legislation. Although they do not solve all legal issues in a perfect manner, they do permit multinational companies to pursue e-discovery exercises without material risks of non-compliance.

[RZ 145]

On the organisational side, the main issue multinational companies usually face is not the clash of (legal) cultures as such, but that they are often not prepared in dealing with it. As a consequence, legal and practical issues such as identifying sources of information are resolved on an ad-hoc basis. The consequence is that legal issues may be addressed too late, time pressure and costs are higher than necessary and know-how in how to best handle e-discovery across the company does not get leveraged for use in other matters. The basic solution to these issues again is a simple one:

Multinational companies should adopt internal structures, procedures and responsibilities that treat e-discovery as a basic corporate function across the entire organisation independent of a particular legal matter. Although not all legal matters in a multinational company will eventually involve cross-border e-discovery, but the number of cases that do will certainly increase. With a corresponding corporate function that is involved early on, that can build up the necessary know-how and experience over time and that can effectively and consistently act as a service center within the organisation for all legal matters, multinational companies will be able to reduce the overall cost and burden of any e-discovery and potentially even use their preparedness as a tactical advantage.

5 Literature

Article 29 Data Protection Working Party, Working Document 1/2009 on pre-trial discovery for cross-border civil litigation, adopted on February 11, 2009.

Hill, Brian W., Owens, Leslie, Searching For eDiscovery Cost Control, Forrester Research, Inc., April 27, 2009.

Kaplan, Ari, Advice from Counsel: Best Practices on Controlling E-Discovery Costs, FTI Consulting, 2009.

Kravitz, Mark R, Memo from Honorable Mark R Kravitz, Chair, Advisory Committee on Federal Rules of Civil Procedure to Honorable Lee H. Rosenthal, Chair, Standing Committee on Rules of Practice and Procedure RE: Report of the Civil Rules Advisory Committee (May 17, 2010).

Logan, Debra, Andrews, Whit, Bace, John, MarketScope for E-Discovery Software Product Vendors, Gartner Report, December 21, 2009.

NIST, US Department of Commerce, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), Special Publication 800–122.

Rosenthal, David, E-discovery in Switzerland: How to deal with DP restrictions, in: Privacy Laws & Business International, October 2007, pp. 9 et seq.

Rosenthal, David, Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zürich 2008.

*The Sedona Conference Working Group 6***,** Comment of The Sedona Conference Working Group 6 to Article 29 Data Protection Working Party Working Document 1/2009 («WP 158»), October 30, 2009.

The Sedona Conference Working Group 6, The Sedona Conference International Principles on Discovery, Disclosure & Data Protection, European Union Edition, Public Comment Version, December 2011.

The Sedona Conference, The Sedona Conference Cooperation Proclamation, The Sedona Conference Journal, Volume 10 Supplement, Fall 2009.

The Sedona Conference, Commentary on Achieving Quality in the E-Discovery Process, May 2009.

Tero,Vivian, Corporate eDiscovery Technology Trends 2009: Doing More with Less While Facing Increasing Complexity in eDiscovery, IDC Information and Data sponsored by FTI Technology, November 2009.

Zeunert, Christian, Kos, Patrick, Daley, James, Rosenthal, David (The Sedona Conference), Working Through the Maze, Part 2: Cross-border Discovery Preparedness & Protocols, 2nd Annual Sedona Conference International Programme on Cross-Border Discovery and Data Privacy, September 15–16, 2010, Washington D.C., USA.

This article is an (updated) translation of a German contribution that first appeared in the German book «Internationale E-Discovery und Information Governance», edited by Prof. Dr. Matthias H. Hartmann, and published by Erich Schmidt Verlag, Berlin, Germany, in 2011 (the German version is freely available from the authors upon request). Christian Zeunert can be reached at Christian_Zeunert@swissre.com and David Rosenthal at david.rosenthal@homburger.ch.

David Rosenthal, Homburger, Zürich, Switzerland
David Rosenthal is counsel and co-head of the IT practice at Homburger, one of the leading Swiss business law firms. He is active in IT and other technology transactions, disputes and regulatory matters as well as in white collar investigations and e-discovery matters. He has published a leading commentary on Swiss data protection law, authored many articles and is a frequent speaker on the topic. He also lectures at the University of Basel Law School and the Federal Institute of Technology in Zürich.

Christian Zeunert, Swiss Reinsurance Company, Zurich, Switzerland
Christian Zeunert is Head E-Discovery Management at Swiss Re, one of the world's leading reinsurers, based in Zurich, Switzerland.
He is responsible for developing, implementing and enforcing Swiss Re's e-discovery strategy and reports to the Claims and legal division. He is a steering board member of The Sedona Conference® Working Group 6 and member of the drafting team of their International Principles on Discovery, Disclosure & Data Protection. Mr. Zeunert is also co-author of a section of the first German speaking book on e-Discovery as well as frequent speaker of e-Discovery conferences.

---

[1]These are the lists of those categories of documents (including ESI) which each party demands from the other as a part of a voluntary pre-trial discovery of documents and information.
[2]One of the toughest sanctions is known as adverse inference, whereby the jury is instructed to presume the documents lost or not disclosed to be unfavourable to the cause of the party which failed to discover or preserve them, in other words, to presume that such documents would corroborate the other party's claims. Among the best-known cases to involve such sanctions is*The Pension Committee of the University of Montreal Pension Plan, et al. v. Banc of America Securities, LLC*, No. 05 Civ. 9016 (SAS), 2010 WL 184312 (S.D.N.Y. Jan. 15, 2010), in which several of the plaintiffs had failed to preserve possibly relevant documents at the time the suit was filed.

[3]An independent European advisory body on matters relating to data protection, established under Art. 29 of EU Data Protection Directive 95/46/EC.

[4]Article 29 Data Protection Working Party, Working Document 1/2009 on pre-trial discovery for cross-border civil litigation, adopted on February 11, 2009, also known as WP 158 (ref. «WP158»), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp158_en.pdf.

[5]The Sedona Conference Working Group 6, *Comment of The Sedona Conference Working Group 6 to Article 29 Data Protection Working Party Working Document 1/2009 («WP 158»), October 30, 2009.*

[6]See footnote 1.

[7]US Federal Rules of Civil Procedure, Rule 26(f).

[8]This refers to the preservation of records as performed in the normal course of business (i.e., conventional records management), in other words before companies are targets of legal action and before their records management is subject to special requirements in connection with the legal action.

[9]Restatement (Third) of Foreign Relations Law of the United States, no. 442.

[10]Cf. *Société Nationale Industrielle Aérospatiale v United States District Court*, 482 U.S. 522, 544 n.28 (1987); *Volkswagen AG v Valdez*, No. 95-0514, 16 November 1995, Texas Supreme Court;*In re: Baycol Products Litigation* MDL no. 1431, 21 March 2003.

[11]See e.g. Art. 271 of the Swiss Penal Code and French Penal Code Law No. 80–538.

[12]Not to be confused with procedural orders such as *scheduling orders* which merely set the timetable for proceedings and thus also define the timing of the parties' discoveries, such disclosures being voluntary rather than compulsory (as when ordered subpoena) under this type of instruction; for a full discussion, see Rosenthal, *Handkommentar zum Datenschutzgesetz*, Zurich 2008 (in German), Art. 271 StGB, N 19 et seq.

[13]Art. 271 of the Swiss Penal Code, which stipulates a penalty of three years' imprisonment or a fine for the individuals in charge.

[14]Including Spain, France and the Netherlands.

[15]As in Swiss law, for example, which in the context of international mutual legal assistance even allows for depositions through a commissioner. In Switzerland, international mutual legal assistance is exempted also from data protection legislation (Art. 2(2)(c) of the Swiss Federal Act on Data Protection).

[16]Which historically has depended largely on how well the parties cooperate, and how well such requests are researched and prepared, on a case-by-case basis.

[17]Examples of such secrecy include professional secrecy (as in Swiss banking secrecy which strictly prohibits disclosing banking client data to entities abroad as there Swiss banking secrecy cannot be guaranteed; another example is Germany's secrecy of telecommunications which is sometimes interpreted to extend even to employees' e-mails stored on their employer's own servers) and contractual secrecy defined so as not to be restricted by civil proceedings and to not allow disclosure even if the parties to the proceedings themselves are bound by secrecy. Whether or not such a clause applies will be a matter of legal interpretation as such rules are rarely drafted with the possibility of a discovery in court proceedings (let alone proceedings abroad) in mind.

[18]Such as in Art. 273 of the Swiss Penal Code or in Art. 124 of the Austrian Penal Code.

[19]Such as redacting certain parts of the text or requesting protective orders.

[20]In the UK the Information Commissioner has the authority to issue fines of up to GBP 500 000 while in Spain fines may be as high as EUR 600 000. In France meanwhile the maximum fine was raised to EUR 150 000 several years ago. In Germany violators may be fined up to EUR 300 000 and in some cases may even face imprisonment.

[21]Art. 139 of the Swiss Federal Law on International Private Law (IPRG); see Rosenthal, footnoteFN 12, Art. 139 IPRG, N 2.

[22]Art. 2 of Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data («EU Data Protection Directive»).

[23]Including in Canada, whose *Personal Information Protection and Electronic Documents Act*establishes that information relating to the name, title, work address and telephone number of an organisation's employee shall not be deemed personal data.

[24]Including in Switzerland, Italy, Austria, Luxembourg and Denmark, among others.

[25]Cf. for example NIST, US Department of Commerce, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), Special Publication 800-122, p. 2-1 (http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf).

[26]The Sedona Conference Working Group 6, The Sedona Conference International Principles on Discovery, Disclosure & Data Protection, European Union Edition, Public Comment Version, December 2011: Principle 5, Comment 6.

[27]Art. 6 and 10 of the EU Data Protection Directive; Art. 4(3) and 4(4) of the Swiss Federal Act on Data Protection.

[28]Art. 7, 11 and 13 of the EU Data Protection Directive; Art. 12(1) and 12(2) and Art. 13 of the Swiss Federal Act on Data Protection.

[29]Art. 6 of the EU Data Protection Directive; Art. 4(2) of the Swiss Federal Act on Data Protection.

[30]WP158, footnote 4.

[31]WP158, footnote 4, p. 12.

[32]WP158, footnote 4, p. 12 ff.

[33]The Sedona Conference Working Group 6, The Sedona Conference International Principles on Discovery, Disclosure & Data Protection, European Union Edition, Public Comment Version, December 2011: Principle 2.

[34]Art. 12 and 14 of the EU Data Protection Directive; Art. 5, 8, 12(2)(b) and 15 of the Swiss Federal Act on Data Protection.

[35]Art. 25 et seq. of the EU Data Protection Directive; Art. 6 of the Swiss Federal Act on Data Protection.

[36]These requirements concern export notification to or export permits from the data protection agencies having jurisdiction in the exporting country (including Austria, Bulgaria, Cyprus, Estonia, Finland, France, Hungary, Iceland, Latvia, Liechtenstein, Lithuania, Malta, Portugal, Romania and Spain, among others).

[37]Such as in Switzerland, where Art. 6(2)(a) of the Federal Act on Data Protection allows companies to conclude any agreements, but also to use other means, to guarantee adequate levels of data protection abroad.

[38]See http://www.export.gov/safeharbor.

[39]Art. 26(1)(d) of the EU Data Protection Directive.

[40]See Chapter 3.4.3 below.

[41]Employees entrusted with managing litigation are referred to as case handlers throughout the remainder of this document.

[42]Among them many members of the Sedona Conference Working Group 6.

[43]At least some companies have started routinely consulting their national e-discovery counsel whenever facing new litigation in the US.

[44]See Chapter 3.2.3.1 below

[45]US Federal Rules of Civil Procedure, Rule 26f. Under the rule, the parties to litigation must, in good faith, confer on any obstacles and issues as may exist in connection with a discovery and resolve these wherever possible, before the formal stage of the discovery begins. The parties should jointly arrive at a plan defining the scope, sequence and form of the disclosure of documents for the purposes of the discovery.

[46]See e.g. the memo from Honourable Mark R Kravitz, Chair, Advisory Committee on Federal Rules of Civil Procedure to Honourable Lee H. Rosenthal, Chair, Standing Committee on Rules of Practice and Procedure RE: Report of the Civil Rules Advisory Committee (May 17, 2010).

[47]See also *The Sedona Conference,* The Sedona Conference Cooperation Proclamation, The Sedona Conference Journal, Volume 10 Supplement, Fall 2009.

[48]See Chapter 3.3.2 below.

[49]As illustrated e.g. in the various publications of the Sedona Conference Working Group 1.

[50]Probably the best-known standard used to define the e-discovery process in the US is the Electronic Discovery Reference Model (EDRM), as detailed at http://edrm.net. See, by contrast, the standard cross border e-discovery procedure followed in Europe (see 3.3.2 below).

[51]Annual Sedona Conference International Program on Cross-Border Discovery and Data Privacy.

[52]Costs will vary case-by-case and in particular according to the data volume (volume times fees) but also depending on the efficiency of the processes used (such as reducing data volumes before reviewing the data manually).

[53]See Chapter 2.2.1 above.

[54]Cf. e.g. Hill/Owens, Searching For eDiscovery Cost Control, Forrester Research, Inc., April 27, 2009; Tero, Corporate eDiscovery Technology Trends 2009: Doing More with Less While Facing Increasing Complexity in eDiscovery, IDC Information and Data sponsored by FTI Technology, November 2009; and Kaplan, Advice from Counsel: Best Practices on Controlling E-Discovery Costs, FTI Consulting, 2009.

[55]See Chapter 2.3.2 above.

[56]See Chapter 3.3.2 below.

[57]Logan/Andrews/Bace, MarketScope for E-Discovery Software Product Vendors, Gartner Report, December 21, 2009

[58]Evaluation performed on systems available in Q1 2011.

[59]While no statistics are available, these statements are supported by information shared among multinationals in relevant industry bodies on e-discovery on the one hand and on the other by empirical evidence from corporate law firms practising in this area in various European countries and in the US.

[60]See The Sedona Conference Working Group 6, The Sedona Conference International Principles on Discovery, Disclosure & Data Protection, European Union Edition, Public Comment Version, December 2011, Appendix C.

[61]WP158, footnote 4.

[62]An efficient way to do this is using specialised software that supports legal-hold workflows. Alternatively, employees may be queried following a conventional interviewing process.

[63]There are exceptions to this rule as well, such as France's data protection legislation which severely restricts the conditions under which employees' personal information may be exported.

[64]A physical solution (i.e., removing the dataset from the physical copy of the database) is not permissible or feasible in every case. In a subsequent civil suit, for example, it may become necessary to adjust the filtering criteria retroactively and disclose a new set of documents. In such cases, the

document in question is simply tagged «irrelevant» or «culled» and will no longer be included in certain search results such as files for export, for instance. Although it will not be disclosed, the document will remain in the early case assessment database of the disclosing party. By contrast, the automated reports generated with the assistance of the relevant filter programs, and the documentations to be prepared manually, should be such that they provide sufficient proof of the accuracy of the culling.

[65]As an example of how such so-called Boolean operators may be applied, consider the exclusionary effect of John NOT (Doe OR Miller OR Smith) and the grouping effect of Alliance AND Star or, alternatively, «Star Alliance». State-of-the-art systems permit even more sophisticated searches, for instance, by requiring that certain search terms are close to each other (e.g., not more than 10 words apart), by automatically searching also for variants of search terms or finding of similar documents.

[66]The Sedona Conference, Commentary on Achieving Quality in the E-Discovery Process, May 2009.

[67]*Da Silva Moore v. Publicis Groupe*, No. 11 Civ. 1279 (ALC) (AJP), 2012 U.S. Dist. LEXIS 23350 (S.D.N.Y. Feb. 24, 2012).

[68]For legal requirements see Chapter 3.4.3 below.

[69]For legal requirements see Chapter 3.4.3 below.

[70]See Chapter 2.2.2.5 above.

[71]Which in the EU are subject to prior review and approval by the data protection agency of the member state concerned if no mutual recognition is possible.

[72]See the lists on http://www.export.gov/safeharbor for data from the EU and from Switzerland.

[73]Commission Decision of December 27, 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, 2004/915/EC, notified under document no. C(2004) 5271.

[74]Commission Decision of February 5, 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and the Council, 2010/87/EC, notified under document C(2010) 593.

[75]A case in point is Art. 11 of the German Federal Data Protection Act (BDSG), under which such transfers are permitted only if done under a detailed outsourcing agreement. Whether the EU standard clauses meet these requirements remains unclear, however, even though they should reasonably be assumed to be compliant. Accordingly, data processing for discovery purposes tends not to be contracted out in Germany.

[76]Rosenthal, footnote FN 12, Art. 6 DSG, N 38.

[77]Art. 6 para. 2 of the Swiss Federal Act on Data Protection.

[78]Commission Decision of July 26, 2000 pursuant to the Directive 95/46/EC of the European Parliament and the Council on the adequate protection of personal data provided in Switzerland, 2000/518/EC, notified under document number C(2000) 2304.

[79]Cf. Chapter 3.4.3 below.

[80]Art. 271 of the Swiss Penal Code; cf. Chapter 2.2.1 above.

[81]For example, see http://www.pacer.gov for public online access to electronic records from US federal appellate, bankruptcy and district courts.

[82]Normally, protective orders provide for two classifications of confidentiality for personal data, «confidential» and «highly confidential» (with restricted access). Personal data as defined under data protection provisions are usually classified as «confidential».