The Sedona Conference Journal

Volume 12 2011

Cross-Border Discovery—Practical Considerations and Solutions for Multinationals

Christian Zeunert & David Rosenthal

Recommended Citation: Christian Zeunert & David Rosenthal, *Cross-Border Discovery—Practical Considerations and Solutions for Multinationals*, 12 SEDONA CONF. J. 145 (2011).

For this and additional publications see:
https://thesedonaconference.org/publications

CROSS-BORDER DISCOVERY – PRACTICAL CONSIDERATIONS AND SOLUTIONS FOR MULTINATIONALS

Christian Zeunert
Swiss Reinsurance Company
Zurich, Switzerland

David Rosenthal
Homburger AG
Zurich, Switzerland

1. Summary

This paper[1] identifies practical considerations for cross-border discovery preparedness and provides a set of protocols that may be used to best comply with applicable Data Protection Laws and U.S. preservation and discovery obligations.

By addressing these issues before litigation is anticipated and again once a specific case is filed, companies are better able to assess the magnitude of cross-border challenges as well as which country specific safeguards need to be implemented, both generally and on a case-by-case basis. A framework is provided here to help companies and their attorneys prepare for early "meet and confer" sessions during which identified cross-border issues can be discussed.

Using a set of existing and adopted protocols in the discovery process, both before and after onwards transfer of personal data, will allow parties to mitigate a number of major cross-border stumbling blocks. Standardized and best centralized e-discovery processes enable the necessary level of education of the attorney-in-charge and ensure that necessary staff in European countries gets involved from the outset of a case.

2. Starting point for multinational companies

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

At the legal level, other than the clashes between the divergent philosophies underpinning the U.S. 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 imperatives 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 U.S. and other countries that – from a European perspective – lack an "adequate" level of protection for personal data.[2]

1 Based on Christian Zeunert, et al., Working Through the Maze Part 2, Cross-border Discovery Preparedness & Protocols, working paper prepared during the 2nd Annual Sedona Conference® International Programme on Cross-Border Discovery and Data Privacy of 15-16 September 2010 in Washington, DC. Special thanks to James Daley and Patrick Kos who contributed to that paper. In addition based on David Rosenthal & Christian Zeunert, E-Discovery und Datenschutz: Herausforderungen und Lösungsansätze für multinationale Unternehmen, Chapter in the first German speaking book on e-discovery "Internationale E-Discovery und Information Governance", Matthias H. Hartmann (Hrsg.), April 2011, http://www.esv.info/download/katalog/media/9783503130740/Leseprobe.pdf.

2 A further English article is planned by the authors to reflect their thoughts on the legal challenges described in the above-mentioned German book chapter.

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 from the individuals who are parties to the dispute, managing the extra time needed to meet the 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.

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.

3. Organizational challenges

3.1 Case-specific and group wide interests

More often than not, the organizational challenges particular to a multinational group involved in a legal case with an 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, adopting an integral, group-wide view only much later, which sometimes may be too late.

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 that 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 U.S. entities.

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 U.S. entities. At many multinationals, this is bound to be a challenge as U.S. e-discovery is often perceived as a matter concerning the U.S. 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 U.S. for flaws in a legal hold and disclosure as part of a pre-trial discovery may long have been one reason why the relevant processes have focused mainly on complying with U.S. procedural law. In more and more cases, however, noncompliance with other countries' legislation on the subject – European law in particular – in connection with conducting an 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).

3.2 The four organizational challenges of an international e-discovery

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:

(a) The first challenge: getting e-discovery experts on board early on

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? Ultimately, this question arises in any litigation that a multinational company finds itself drawn into in the U.S. Answering it is likely, at first, to baffle most individuals tasked with handling such cases.[3] 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 U.S. Their expertise will be of a different sort: either they are in-house counsels with more or less experience in litigation and some knowledge of applicable U.S. 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.

Actual experience shows that such case handlers may not know the correct questions, never mind the legal, organizational and technical requirements involved in securing and obtaining evidence outside the U.S., 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.

Absolutely key to preparing for any anticipated U.S. 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 third-party U.S. trial lawyers usually mandated to represent them in a specific case are not the ideal partners to contact in such cases:

For one thing, many U.S. 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 U.S. borders. It is true that more and more big U.S. 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.[4] 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.[5] For another, third-party lawyers typically are unfamiliar with the specific situation at the company with regard to the areas relevant to an e-discovery.

3 Employees entrusted with managing litigation are referred to as case handlers throughout the remainder of this document.
4 Among them many members of The Sedona Conference® Working Group 6.
5 At least some companies have started routinely consulting their national e-discovery counsel whenever facing new litigation in the U.S.

This is because in multinational companies, which tend to contract external lawyers 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.

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 U.S. at all.

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. For this is also the onset, under the U.S. Federal Rules of Civil Procedure, of the company's duty to preserve any documents and data that may be relevant to the litigation, and the company must employ the organizational and technological resources necessary in ensuring that no potential evidence can be destroyed from that moment on.

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 U.S. litigation, which, by its very nature, most times starts out with an U.S. 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[6] before the actual discovery has even begun and to change tracks if and as necessary.

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,[7] 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 U.S. 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.

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 are highly likely, neither of them desirable. One, that any risk assessment that might be adequate from a company or case perspective will fall by the wayside, at the expense of compliance with data protection laws and other non-U.S. legal requirements. Two, that the company will find itself unable to honor the protocols established in the meet-and-confer.

---

6 *See* 8.2, *infra*.

7 FED. R. CIV. P. 26(f). 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.

(b) The second challenge: educating, and working together

In Europe as well as the U.S., 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 U.S. 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.

Sadly, experience suggests that the vast majority of U.S. 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 U.S. 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[8] and more and more training programmes are coming on stream there to address it.[9] Concomitant with this, U.S. 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.

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.

Sadly, experience shows that the U.S. Federal Rule of Civil Procedure 26(f) dated back to December 2006 is not yet standard practice with all U.S. 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. 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 trial 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 trial. 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 U.S. The company needs to have done this so it can educate its external U.S. 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

8 *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 (17 May 2010).

9 Such as the free yet high-quality training available through The Law Institute.

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.

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 select, quasi "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 various "preferred" 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 costs of any subsequent e-discovery.

(c) The third challenge: time-consuming additional measures

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.

In practice, one approach that has proven useful has the parties agree on phased discovery, starting with the – typically straightforward – U.S. 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 U.S. and especially from Europe.

(d) The fourth challenge: compliance in practice

Yet another practical challenge facing multinational companies is to be meticulous enough in complying with the e-discovery requirements under U.S. law.[10] 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 an e-discovery takes on a cross-border dimension, with a raft of additional requirements as described above, implementing the rules becomes even more challenging.

One of the difficulties routinely facing multinationals is that the processes[11] developed by the industry bodies and experts – and the tools (software solutions) to implement them – often cater only to the U.S. 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.

10 As illustrated, e.g., in the various publications of The Sedona Conference® Working Group 1.

11 Probably the best-known standard used to define the e-discovery process in the U.S. 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* 8.2, *infra*).

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.

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.

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.

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 semi-automated 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 U.S. 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.

4. Workable solutions for multinational companies

4.1 Introductory remarks

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 U.S. law and European data protection legislation as well as other applicable legal requirements.

On closer inspection, 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 become the subject of discussions being held at the relevant international bodies, including The Sedona Conference®,[12] 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:

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 U.S. 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 as much as USD 0.5-3 million.[13]). 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 U.S. There is hardly a European group or group headquarters not prepared to assist its U.S. subsidiary in a local dispute if reasonably able to do so. Nor should the influence of legal advisors be underestimated: whenever a European firm finds itself involved in some legal action in the U.S., 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 U.S. tradition.) Refusing disclosure is virtually unthinkable for U.S. 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 documents reviewed as part of a discovery, against their client's will if necessary, also to cover themselves.

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 U.S. 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, U.S. 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-

12 Most recently at the 3rd Annual Sedona Conference® International Programme on Cross-Border Discovery and Data Privacy held in Lisbon, Portugal, 22-23 June 2011.

13 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).

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 U.S. 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 U.S. 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 U.S. these days expect multinationals to be aware of the e-discovery scenarios they may face down the road, and to prepare accordingly.

Third, 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. While not a given, 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 of defendant companies or a defendant group. This role involves ensuring that those representing the different legal cultures – that is, the mandated third-party lawyers – all 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 talks in a given case. In their external relations as well, companies are well advised to be proactive about educating the court of jurisdiction and their opponent on the requirements under European 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-U.S. jurisdictions. Even today, the duty to ensure such awareness in U.S. civil suits rests squarely on the shoulders of the defendant company, despite the growing appreciation in the U.S. in recent years of the challenges posed by European data protection laws.

(a) Understanding the company's own particular situation

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.

Thus, any firm that intends to assess internally the likely scope and consequences of a cross-border e-discovery in specific U.S. 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. As shown time and again above, it is indispensable for a company to understand its own particular situation before going into meet-and-confer talks with the counterparty at the start of a U.S. 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 databases 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.

Following below, this text 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-discovery. 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.

(b) Organisational aspects particular to multinationals

First a company should know how and where its value chain is managed. In many multinationals this process is spread across different countries. Accordingly, research and development, 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.

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; while the department head may be based in one location, some of his or her direct reports may be spread over two, three or more locations.

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.

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 an e-discovery and allow monitoring for this purpose.

(c) IT aspects particular to multinationals

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 by region and bundle it in one single country. And company database management trends are moving in the same direction.

Among other things, these trends have been gradually eroding any prior strict separation of U.S.-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.

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

Next, the firm should collect information on and document where it physically stores 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 an e-discovery. 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 firm 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.

(d) How to analyze cross-border e-discovery in a multinational firm

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

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.

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?

At a second stage the multinational must find out where the expected U.S. court trial will be held and according to what rules. Even within the U.S. the rules, standards and practices that apply to e-discovery 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.

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 U.S., given the documents subject to discovery and the applicable provisions of U.S. 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 firm 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 firm whose remit includes these ancillary measures and if government agencies (such as national data protection agencies) must be involved.

5. Accepting pragmatic compromises

5.1 Preliminary remarks

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

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 – anonymity and assigning pseudonyms to all discoverable data prior to discovery, in fact even prior to transmission to a third-party 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.

By contrast, were a discovery run in the classic U.S. tradition, the data collected as part of an e-discovery would be reviewed only for legally privileged content, if at all, before disclosure. It would not involve any measures to protect the privacy of employees, for instance, as under U.S. 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 where such use results in their public disclosure.

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 satisfying depending on the interpretation of applicable data-protection legislation.

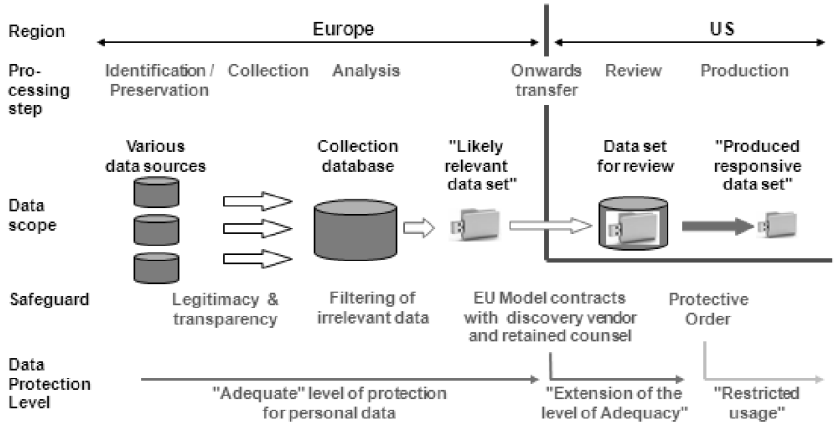
5.2 Standard procedure for conducting cross border e-discovery in Europe

In and of itself, recognizing the conflict between European data protection laws on the one side and U.S. 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-discovery in their European operations as well. Inevitably, they need to strike some kind of compromise.

In response to these conditions a standard procedure evolved in recent years for e-discovery 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.[14] Various versions of the procedure have been described in the literature and discussed in specialist bodies.

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[15]) by this body and merely represents a (useful) compromise. Quite likely, however, it is this very approach – prizing usability over perfection – that accounts for the procedure's success.

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

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:

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. Following the written legal hold notice, the employees are given a questionnaire asking them to identify the systems on which they have been storing any documents and information potentially relevant to the case at hand.[16] 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 terms of the company systems familiar to them, the employees should be asked to be as precise as possible in identifying the area that is potentially relevant in their view. For

14 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.

15 Article 29 Data Protection Working Party, Working Document 1/2009 on pre-trial discovery for cross border civil litigation, 00339/09/EN (WP 158).

16 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.

instance, they should indicate the folders they have been using for storing files on their local hard drives and network drives 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 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 personal content: employees are reminded either that in line with applicable company regulations, personal content may not be stored at all or only in specific locations (such as dedicated directories on employees' local hard drive, the data in which are not collected for e-discovery purposes) or to remove their personal data in good time lest these be included in the data subject to the discovery.

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.[17] If the company in question already has a solution in place for archiving the data (such as e-mails) 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 features, filters and export interfaces. Inevitably, this database will include large quantities of irrelevant information and possibly personal data as well. Whether using a proprietary system or an archiving solution, the company must ensure that no data can illegally or unintentionally be deleted, modified or lost. (If using an archiving solution in parallel, the company must ensure in particular that the feature that automatically deletes documents upon the end of their defined archiving period – frequently the default setting – is turned off, so that documents for relevant custodians are archived indefinitely). Therefore, but also for data protection reasons, access rights to the data backed up 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.

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.[18] The data culling is performed manually, whereby e-discovery experts

17 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.

18 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.

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, or 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 terms of exclusion (operator "NOT") and grouping keywords (operator "AND").[19] For obvious reasons, search runs are often started with very broad keywords, such as general descriptive terms, first 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 keywords, 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 U.S. as well.[20] 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. 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.

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 U.S. or is made available to these by remote access to the review system of an e-discovery provider in the U.S. or in Europe.[21] 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 U.S. Yet experience shows that with remote access, costs are up to 50% higher than if a U.S.-based e-discovery provider is used. At the same time, these authors do not consider the European option, with remote access from the U.S., to be essential. To be sure, it is still cheaper than flying in U.S. lawyers to review documents, which would be unreasonable to do purely for the sake of data protection.

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 personal or otherwise irrelevant files. That said, proper culling requires that the individuals tasked with reviewing the files

19 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".

20 THE SEDONA CONFERENCE , THE SEDONA CONFERENCE , COMMENTARY ON ACHIEVING QUALITY IN THE E-DISCOVERY PROCESS (May 2009).

21 For legal requirements, *see* chapter 8.3 below.

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 personal (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.

Whether it is sufficient to cull the personal 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.

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).

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 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 anonymity of persons' names now tends to be interpreted as a recommendation rather than an obligation.

At a fifth and final stage the data manually reviewed and (where necessary) redacted during the fourth stage are disclosed by the U.S.-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.[22]

22 For legal requirements see chapter 8.3 below.

5.3 Safeguards for onward transfer and disclosure

(a) EU Model clauses and alternatives

The data protection directive (95/46/EC) establishes the principle in Article 25(1) that transfers of personal data to third countries should only take place where the third country in question ensures an adequate level of protection. Article 26 sets out certain exemptions to that rule.

According to Working Paper (WP) 158 none of the exemptions provided in Article 26(1) are feasible with respect to a U.S. e-discovery request.[23] However, one comment regarding Article 26(1)(a) "consent" may be made. The reasoning provided in WP 158 may be true concerning "blue collar" and lower and mid-level management employees, however, if a custodian is part of the high-level management, this may differ in specific situations where the custodian may have a real choice to consent or to oppose to the transfer of his personal data which may endanger his privacy rights, e.g., if the custodian is in a senior management position. Therefore, if a company has processes in place which ensure the possibility for a custodian to review a data set which is in scope of a U.S. e-discovery request and which includes the custodian's personal data so the custodian's privacy rights are protected, such approach may qualify as feasible and may provide legitimacy of processing of the data at hand for litigation purposes.

Further, additional possibilities for exemption from the "adequate protection" principle of Article 25 are set out in Article 26(2). This provision allows an EU member state to authorize a transfer or set of transfers to a "non-adequate" third country "where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights". Despite the various options provided in Article 26(2) for complying with the data protection directive, many of the mechanisms have either limited or no utility in many circumstances. For example, most financial services companies are not eligible to participate in the Safe Harbor program. Further, Binding Corporate Rules (BCRs) appear to be "off the shelf" solutions to international transfers and there is currently no fast-track method for obtaining Data Protection Authorities approval applying to all member states. In addition, BCRs may be applied within one corporate group of companies only but not in connection with third party vendors, such as outside legal counsel or e-discovery service providers. Eventually, Data Protection Authorities may subsequently audit companies and find the enforcement of BCRs to be inadequate.[24]

From a practical standpoint it may depend whether it makes sense that an EU based company which is exposed to U.S. litigations may prepare agreements based on Standard Contractual Clauses III (controller-to-processor), II (controller-to-controller) or the engagement letter with data protection clauses.[25] Such agreements are at hand once a U.S. e-discovery requests pops up and European data need to be provided to the U.S. on short notice. Further, it is advisable to contact potential third party services providers and

23 Article 29 Data Protection Working Party, Working Document 1/2009 on pre-trial discovery for cross border civil litigation, 00339/09/EN (WP 158), 6 ff.

24 Data Protection Directive, Article 26(2). BCRs are a set of rules adopted within a particular company or corporate group that provide legally binding protections for data processing within the company or group. BCRs can be legally binding on members of a corporate group through a variety of legal devices and may provide a legal basis for data transfers to other countries or regions. Most multinational corporations use BCRs for a variety of compliance requirements such as environmental, health and safety, money laundering, and general corporate governance requirements.

25 For example, *see* the template of an insert for engagement letters containing data protection language to be used when companies in Switzerland retain US counsel, a copy of which is attached as Appendix 2 (template provided by David Rosenthal, Homburger AG).

outside counsel prior to a litigation and advice on the general necessity of signing Standard Contractual Clauses and to discuss potential questions related to the processes on how the data shall be provided and what data privacy security measures must be implemented once a litigation becomes actual where European data may be required for e-discovery purposes.

(b) Confidentiality agreements and court-approved protective orders

Confidentiality agreements and court-approved protective orders can help protect the security and integrity of protected data that is being processed and/or transferred in the context of In U.S.-based litigation and regulatory investigations. They are important tools for helping navigate the divide between data privacy and U.S.-based discovery and disclosure.

Within the context of U.S. litigation and regulatory discovery and disclosures, confidentiality agreements are used in a wide variety of information contexts to protect sensitive information. Confidentiality agreements between the parties are often put in place very early because they do not require the time and cost of court intervention, thereby expediting the discovery process.

U.S. federal courts (as well as most U.S. state courts) provide a procedural scheme for implementing confidentiality agreements through a mandatory meet-and-confer process. This process requires parties to meet very early and, if possible, to reach agreement on a discovery plan that includes measures regarding handling of confidential, trade secret, and other proprietary information.[26] The discovery plan must consider "any issues about disclosure or discovery of electronically stored information" as well as "any issues about claims of privilege or of protection as trial-preparation materials, including — if the parties agree on a procedure to assert these claims after production — whether to ask the court to include their agreement in an order."[27] The parties may seek a protective order in order "to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense." This option is often sought where discovery involves the exchange of very sensitive information which, if made public, could cause irreparable harm or damage. For good cause shown, the court can issue a protective order that forbids certain discovery or limits it by time, manner, place, and/or cost.[28]

Unlike a confidentiality order, a protective order requires one or more of the parties to file a motion with the court, with the accompanying additional time, cost and expenditure of already scarce judicial resources. These burdens are especially high when such a motion is contested. The burdens are considerably less when the parties merely desire the court to give its blessing in a "Joint and Stipulated Confidentiality and Protective Order."

One reason that a protective order is often preferred in the case of sensitive information is that U.S. procedure rules provide a more efficient enforcement scheme for court orders than for confidentiality agreements. Indeed, failure to obey a court order can subject a party to sanctions under Federal Rule of Civil Procedure 37(b)(2), while breach of a confidentiality agreement is often treated as a matter of contract law, requiring additional legal steps before it can be enforced.

Where protected data needs to be processed and/or transferred across borders in the context of U.S.-based discovery and disclosure, parties should seek, and courts and

26 FED. R. CIV. P. 26(f).
27 FED. R. CIV. P. 26(f)(3)(C) and (D).
28 FED. R. CIV. P. 26(c)(1).

regulators should grant a specific Confidentiality and Protective Order for Protected Personal Data. The parties can initially execute a confidentiality agreement, and then seek a Joint and Stipulated Confidentiality and Protective Order. Court-approved Case Management Orders should include a standard provision for the confidentiality of protected data. From the perspective of data protection and privacy advocates, a court-approved protective order is preferred over a confidentiality agreement for several reasons. First, it establishes a stronger sense of management and accountability for the protected data. If the court is directly involved, there is a stronger expectation that provisions relating to personal data will be honored. Second, it provides a built-in enforcement mechanism — a major consideration of any cross-border data protection scheme, including Safe Harbor.

On the one hand, U.S. courts and regulatory agencies acting in their adjudicative capacity may be reluctant to endorse the broad use of protective orders for processing and transfer of protected data because it requires the expenditure of scarce judicial resources. The thought might be that if the parties can reach their own confidentiality agreement, why does the court need to be involved? On the other hand, a U.S. court order regarding protected data can engender substantial trust and confidence outside the U.S. because it signals that legitimate data privacy concerns are recognized and respected. It is, moreover, a sign of respect and comity as well. A protective order of the type attached as Appendix 3 can help bridge the divide between the competing interests of data privacy and protection and U.S.-based discovery and disclosure compliance. They can be an important tool in safely navigation the maze of cross-border discovery.

Appendix 1: CROSS-BORDER DISCOVERY ANALYSIS
Set of questions assessing the cross-border exposure and country specific requirements

1. Organizational & IT check

(a) *Globalization*: Does the company operate globally and does it have a globalized process chain? Does the company respectively the departments/units at issue operate in global teams?

(b) *Off-/near-shoring or outsourcing*: Does the company make use of off-/near-shoring or outsourcing for particular business processes at issue?

(c) *Data Separation:*[29] Has a strict separation between U.S. data and other countries' or regions' data been implemented? If yes, for part or for all systems & data?

(d) *Global Data Flow:* Does the data flow at a global level within the company and, if so, how? For which business processes?

(e) *Cross-border data access:* Can the data be accessed cross-border and globally in the ordinary course of business?

(f) *Access controls:* How is it implemented - generally or per (relevant) systems?

(g) *Data ownership:* How is the concept of data controller/processor implemented?

(h) *Data hubs*: Has IT centralized the data in regional hubs, e.g., in the U.S., Europe and Asia? If yes, which countries belong to which data hub? Which business processes are organized in those data hubs?

(i) *Cloud computing:*[30] Does IT make use of cloud computing? If yes, how is cloud computing implemented, e.g., is a European cloud used for European data?

(j) *Service provision:* Is IT provided internally, by an outside service provider or through a combination of both?

2. General fact finding

(a) Venue,[31] type[32] and parties[33] of the proceeding?

(b) Geographic[34] and legal entity[35] scope of custodians and data sources?

29 Data, which are either physically or via restrictive access controls organized in a way, that the data can only be viewed and modified by staff of certain country/countries excluding specific other countries, e.g., HR data managed separately in Germany with no access controls for U.S. staff.

30 Cloud concepts vary heavily: from "private clouds" with dedicated server for one company hosted in Europe to a "pure cloud" with unspecified servers around the globe.

31 **The venue** of the proceeding for the scope of this paper and conference is the U.S. The scope of discovery as well as the process varies in the different common law countries.

32 **The type of proceeding** (litigation, arbitration, formal governmental investigation, informal cooperation with government) may in certain countries (e.g., Switzerland) impose mandatory restrictions on a willingly cooperating party before evidence gathering and disclosure can be done.

33 **The parties to the proceeding**: In cross-border cases one needs to clarify which legal entity is part of the proceeding and whether additional legal entities fall within the scope of the data preservation and collection. This clarification will also be relevant in the light of Article 271 Swiss Penal Code, given that the voluntary provision by a party of its own data in U.S. litigation may be performed subject to implementation of adequate data protection safeguards.

34 **The geographic scope** will determine country specific data protection requirements and in particular if and under which circumstances data may be exported.

35 **The legal entity scope**: A legal entity in country A may still be the data controller although the data are physically stored in country B. Clarification may be needed as to which data protection law applies with regard to the processing of the data and, therefore, which country's data protection law may apply.

(c) Type of custodians[36] and persons affected (e.g., current employees, former employees, third parties)?

(d) Nature of data at issue (non-personal, personal[37] or sensitive personal data or other restricted[38] data)?

(e) The type of custodian and persons affected may also be relevant for determining applicable law?

3. Country and case specific safeguard check:

(a) Which policies, if any, govern the preservation, collection, review, disclosure and other cross-border transfer activities within the legal entities at issue?

(b) Which safeguards need to be implemented for which country, data category and activity at which point in time?

(c) Do the custodians need to be informed / give consent prior to processing?

(d) Does the affected party or affiliate need to involve any officials or specific persons, e.g., data protection authority, data protection officer or works council?

(e) Does any treaty or agreement need to be followed or implemented (e.g., Hague Convention, EU model contracts, protective order, confidentiality agreement, etc.)?

(f) Are there other specific safeguards to be implemented prior to the preservation, collection, review and disclosure (e.g., specific review procedures, special privacy reviews or remote access for cross-border data access)?

(g) Is it necessary to involve the respective data protection authority?

(h) Is the Hague Convention or an alternative process for exporting available in the specific case?

(i) Should privacy measures such as anonymity or having a pseudonym for` personal data such as email addresses and names in e-mails be employed?

(j) What are the sanctions in case of non-compliance with applicable data protection laws and how strictly are such laws enforced?

(k) Verify legitimacy of data processing (does the purpose warrant the infringement of privacy every discovery will cause, even if limited to business data of employees?).

(l) Ensure transparency to the data subjects.

(m) Filter private and other irrelevant personal data prior to the onward transfer to another jurisdiction (without adequate level of data protection).

---

36 **The type of custodian** and persons affected may trigger the need to comply with additional legal restrictions, such as employment law or specific secrecy obligations (e.g., in case of secrecy undertakings vis-à-vis certain customers). The type of custodian and persons affected may also be relevant for determining applicable law.

37 **Personal data** is in principle defined in the EU Directive, but its definition may vary per country. The context of personal data may raise practical considerations on whether data protection law applies at all and which safeguards need to be implemented to achieve reasonableness, proportionality and to avoid overriding the fundamental rights and freedoms of data subjects.

38 **Sensitive personal as well as restricted data** fall into a special category of processing.

Appendix 2: MODEL DATA PROTECTION LANGUAGE FOR CLIENT ENGAGEMENT LETTER

We are aware that data protection laws of Switzerland and the countries of the European Union (the **Data Protection Laws**) regulate the collection, use, disclosure, storage, export and other processing (as defined in the Data Protection Laws) of personal data. In light of these Data Protection Laws we agree to the following provisions (the **Data Protection Provisions**):

[LAWFIRM]'s collection, use, disclosure, storage, export and other processing of personal data (as defined in the Data Protection Laws) provided to, or obtained by, [LAWFIRM] by or on behalf of [CLIENT] (the **Data**) will be conducted solely on behalf of, and solely for the purposes of, [CLIENT], only in accordance with any instructions provided by [CLIENT] (including without limitation instructions of [CLIENT] for the purpose of compliance with inquires and requests of data subjects concerning their right of information, correction, blocking, suppression or deletion of Data), and pursuant to appropriate technical and organizational measures as required by the Data Protection Laws to protect the Data from unauthorized processing, including any processing not expressly authorized by this Agreement and including accidental loss or destruction of, or damage to, such Data. [LAWFIRM] will not subcontract or delegate its processing of Data to a third party or to a country other than Switzerland or European Union member state without prior written consent of [CLIENT]. Also, [LAWFIRM] will refrain from further processing Data and return (and destroy any copies) of Data if and when requested so by [CLIENT]. The obligations of [LAWFIRM] set forth in the foregoing sentence shall also apply in the case of a termination of the engagement or the engagement letter and shall survive any such termination for whatever reasons. The firm will not disclose any documents to any other person or entity (including without limitation public authorities) without the express permission of [CLIENT]. [LAWFIRM] will promptly inform, and cooperate with, [CLIENT] if it believes that it may no longer be able, or no longer is able, to comply with these Data Protection Provision or if any accidental or unauthorized access has occurred. [CLIENT] has the right in any reasonable manner and with [LAWFIRM]'s full cooperation, audit [LAWFIRM]'s compliance with these Data Protection Provisions or to have such audit performed by a qualified third party bound by a duty of confidentiality. [LAWFIRM] will cooperate with [CLIENT] if, in [CLIENT]'s reasonable interpretation, additional steps are required for compliance with the Data Protection Laws or other applicable data protection laws.

Appendix 3: PROPOSED DRAFT LANGUAGE[39] FOR U.S. CONFIDENTIALITY AND PROTECTIVE ORDER GOVERNING PROTECTED DATA

1. This Protective Order shall govern the use of all Protected Materials produced by, or on behalf of, any Litigant. Notwithstanding any order terminating this proceeding, this Protective Order shall remain in effect until specifically modified or terminated by the Court.

2. This Protective Order applies to the following two categories of materials: (a) Personal Data, as defined in the EU Data Directive 95/46, which includes any personally identifiable information that has been processed and transferred to the United States for the purpose of responding to discovery requests in this litigation; and (b) Personal Sensitive Data, as defined in the EU Data Directive 95/46, which includes any personally identifiable information regarding a person's health, finances, personal background, family and the like that has been processed and transferred to the United States for the purpose of responding to discovery requests in this litigation. All Litigants shall designate and mark such materials as "EU PROTECTED MATERIALS" or "EU PROTECTED SENSITIVE MATERIALS," respectively.

3. Definitions – For purposes of this Order:

   (a) The term "Litigant" shall mean a party litigant, or third-party, from whom Protected Materials are sought for the purpose of this matter.

   (b) The term "Protected Materials" means (i) all materials provided by a Litigant in response to discovery requests and designated by such Litigant as protected; (ii) any information contained in or obtained from such designated materials; (iii) any other materials made subject to this Protective Order by the Court, by any court or other body having appropriate authority, or by agreement of the Litigants; (iv) notes regarding Protected Materials; and (v) copies of Protected Materials. The Litigant producing the Protected Materials shall physically mark them on each page as "EU PROTECTED MATERIALS."

   (c) The term "Notes Regarding Protected Materials" means memoranda, handwritten notes, or any other form of information (including electronic form) which copies or discloses materials described in Paragraph 5. Notes Regarding Protected Materials are subject to the same restrictions provided in this order for Protected Materials, except as specifically provided in this order.

   (d) The term "Non-Disclosure Certificate" shall mean the certificate annexed hereto by which Litigants who have been granted access to Protected Materials shall certify their understanding that such access to Protected Materials is provided pursuant to the terms and restrictions of this Protective Order, and that such Litigants have read the Protective Order and agree to be bound by it. All Non-Disclosure Certificates shall be served on all parties on the official service list maintained by the Clerk in this proceeding.

   (a) The term "Reviewing Representative" shall mean a person who has signed a Non-Disclosure Certificate and who is:

39 By M. James Daley, CIPP, Daley & Fey LLP.

1. Court Clerk or Court Staff;

2. An attorney who has made an appearance in this proceeding for a Litigant;

3. Attorneys, paralegals, and other employees associated for purposes of this case with an attorney described in Paragraph (2);

4. An expert or an employee of an expert retained by a Litigant for the purpose of advising, preparing for, or testifying in this proceeding;

5. A person designated as a Reviewing Representative by order of the Court; or

6. Employees or other representatives of Litigants appearing in this proceeding with significant responsibility for this docket.

4. Protected Materials shall be made available under the terms of this Protective Order only to Litigants and only through their Reviewing Representatives as provided below.

5. Protected Materials shall remain available to Litigants until the later of the date that an order terminating this proceeding becomes no longer subject to judicial review, or the date that any other judicial proceeding relating to the Protected Material is concluded and no longer subject to judicial review. If requested to do so in writing after that date, the Litigants shall, within fifteen (15) days of such request, return the Protected Materials (excluding Notes of Protected Materials) to the Litigant that produced them, or shall destroy the materials, except that copies of filings, official transcripts and exhibits in this proceeding that contain Protected Materials, and Notes of Protected Material may be retained, if they are maintained in accordance with this Order. Within such time period each Litigant, if requested to do so, shall also submit to the producing Litigant an affidavit stating that, to the best of its knowledge, all Protected Materials and all Notes of Protected Materials have been returned or have been destroyed or will be maintained in accordance with this Order. To the extent that Protected Materials are not returned or destroyed, they shall remain subject to the Protective Order.

6. All Protected Materials shall be maintained by the Litigant in a secure place. Access to those materials shall be limited to those Reviewing Representatives specifically authorized by this Order. The Clerk shall place any Protected Materials filed with the Court in a non-public file. By placing such documents in a non-public file, the Court is not making a determination of any claim of privilege. The Court retains the right to make determinations regarding any claim of privilege and the discretion to release information necessary to carry out its responsibilities.

7. Protected Materials shall be treated as confidential by each Litigant and by the Reviewing Representative in accordance with the certificate executed pursuant to this Order. Protected Materials shall not be used except as necessary for the conduct of this proceeding, nor shall they be disclosed in any manner to any person except a Reviewing Representative who is engaged in the conduct of this proceeding and who needs to know the information in order to carry out that person's responsibilities in this proceeding. Reviewing Representatives may make copies of Protected Materials,

but such copies shall become Protected Materials. Reviewing Representatives may make notes of Protected Materials, which shall be treated as Notes of Protected Materials if they disclose any portion of the contents of Protected Materials.

8. In the event that a Litigant wishes to designate as a Reviewing Representative a person not described in Paragraph 3(e) above, the Litigant shall seek agreement from the Litigant providing the Protected Materials. If an agreement is reached, that person shall be treated as a Reviewing Representative pursuant to Paragraphs 3(e) above with respect to those materials. If no agreement is reached, the Litigant shall submit the disputed designation to the Court for resolution.

9. A Reviewing Representative shall not be permitted to inspect, participate in discussions regarding, or otherwise be permitted access to Protected Materials pursuant to this Protective Order unless that Reviewing Representative has first executed a Non-Disclosure Certificate, provided that if an attorney qualified as a Reviewing Representative has executed such a certificate, the paralegals and secretarial and clerical personnel under the attorney's instruction, supervision, or control need not do so. A copy of each Non-Disclosure Certificate shall be provided to counsel for the Litigant asserting confidentiality prior to disclosure of any Protected Material to that Reviewing Representative. Attorneys qualified as Reviewing Representatives are responsible for ensuring that persons under their supervision or control comply with this order.

10. Any Reviewing Representative may disclose Protected Materials to any other Reviewing Representative as long as the disclosing Reviewing Representative and the receiving Reviewing Representative both have executed a Non-Disclosure Certificate. If any Reviewing Representative to whom the Protected Materials are disclosed ceases to be engaged in these proceedings, or is employed or retained for a position whose occupant is not qualified to be a Reviewing Representative, access to Protected Materials by that person shall be terminated. Even if no longer engaged in this proceeding, every person who has executed a Non-Disclosure Certificate shall continue to be bound by the provisions of this Protective Order and the certification.

11. Subject to Paragraph 17, the Court shall resolve any disputes arising under this Protective Order. Prior to presenting any dispute under this Protective Order to the Court, the parties to the dispute shall use their best efforts to resolve it. Any Litigant that contests the designation of materials as protected shall notify the party that provided the Protected Materials by specifying in writing the materials whose designation is contested. This Protective Order shall automatically cease to apply to such materials five (5) business days after the notification is made unless the designator, within said 5-day period, files a motion with the Court, with supporting affidavits, demonstrating that the materials should continue to be protected. If any challenge to the designation of materials as protected is made, the burden of proof shall be on the Litigant seeking protection.

12. All copies of all documents reflecting Protected Materials, including relevant portions of the hearing testimony, exhibits, transcripts, briefs, and other documents which refer to EU Protected Materials, shall be filed and served in sealed envelopes or other appropriate containers endorsed to the effect that they are sealed pursuant to this Protective Order. Such documents shall be marked "EU PROTECTED MATERIALS" and shall be filed under seal and served under seal upon the Court and

all Reviewing Representatives who are on the service list. Such documents containing personal sensitive data shall be additionally marked "Contains EU PROTECTED SENSITIVE MATERIALS."

Where anything is filed under seal, redacted versions of the materials—or, where an entire document is protected, a letter indicating such—will also be filed with the Court and served on all parties on the service list and the Court. Counsel for the producing Litigant shall provide to all Litigants who request the same a list of Reviewing Representatives who are entitled to receive such material. Counsel shall take all reasonable precautions necessary to assure that Protected Materials are not distributed to unauthorized persons. If any Litigant desires to include, utilize, or refer to any Protected Materials or information derived therefrom in testimony or exhibits during any hearing or trial in these proceedings in such a manner that might require disclosure of such material to persons other than Reviewing Representatives, such Litigant shall first notify both counsel for the disclosing Litigant and the Court of such desire, identifying with particularity each of the Protected Materials. Thereafter, use of such Protected Material will be governed by procedures determined by the Court.

13. Nothing in this Protective Order shall be construed as precluding any Litigant from objecting to the use of Protected Materials on any legal grounds.

14. Nothing in this Protective Order shall preclude any Litigant from requesting the Court, the Court, or any other body having appropriate authority, to find that this Protective Order should not apply to all or any materials previously designated as Protected Materials pursuant to this Protective Order. The Court may alter or amend this Protective Order as circumstances warrant at any time during the course of this proceeding.

15. Each party governed by this Protective Order has the right to seek changes in it as appropriate from the Court or the Court.

16. All Protected Materials filed with the Court, the Court, or any other judicial or administrative body, in support of, or as a part of, a motion, other pleading, brief, or other document, shall be filed and served in sealed envelopes or other appropriate containers bearing prominent markings indicating that the contents include Protected Materials subject to this Protective Order. Such documents containing personal sensitive data shall be additionally marked "Contains EU PROTECTED SENSITIVE MATERIALS."

17. If the Court finds at any time in the course of this proceeding that all or part of the Protected Materials need not be protected, those materials shall, nevertheless, be subject to the protection afforded by this Protective Order for three (3) business days from the date of issuance of the Court's decision, and if the Litigant seeking protection files an interlocutory appeal or requests that the issue be certified to the Court, for an additional seven (7) business days. None of the Litigants waives its rights to seek additional judicial remedies after the Court's decision respecting Protected Materials or Reviewing Representatives, or the Court's denial of any appeal thereof.

18. Nothing in this Protective Order shall be deemed to preclude any Litigant from independently seeking through discovery in any other administrative or judicial proceeding information or materials produced in this proceeding under this Protective Order.

19. None of the Litigants waives the right to pursue any other legal or equitable remedies that may be available in the event of actual or anticipated disclosure of Protected Materials.

20. The contents of Protected Materials or any other form of information that copies or discloses Protected Materials shall not be disclosed to anyone other than in accordance with this Protective Order and shall be used only in connection with this (these) proceeding(s). Any violation of this Protective Order and of any Non-Disclosure Certificate executed hereunder shall constitute a violation of an order of the Court.

SO ORDERED.

Court_____

IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF

Name of case

Docket No.

NON-DISCLOSURE CERTIFICATE

I hereby certify my understanding that access to Protected Materials is provided to me pursuant to the terms and restrictions of the Protective Order in this proceeding, that I have been given a copy of and have read the Protective Order, and that I agree to be bound by it. I understand that the contents of the Protected Materials, any notes or other memoranda, or any other form of information that copies or discloses Protected Materials shall not be disclosed to anyone other than in accordance with that Protective Order. I acknowledge that a violation of this certificate constitutes a violation of an order of the Court.

By:_____

Title: _____

Representing: _____

Date: _____