

# Global electronic discovery: an introduction to European electronic stored information (ESI) collection and production

8 November 2009  
Gregory Bufithis, Esq.



*Preface:* If we are to believe the prognosis of many economists, the current recession is on the verge of ending. The rebounding economy will most likely re-invigorate corporations to push their markets globally. This, in turn, will further push litigation and regulatory enquiries globally.

The best prepared corporations will have a litigation readiness and response plan in place that adheres to the European Union Directives and other information management and discovery protocols. It is no longer a question of “*if*” litigation support professionals need to be prepared for discovery requests that go beyond US borders; it is a question of “*when*”.

It is necessary for U.S. companies to understand the legal complexities of collecting, culling and reviewing data from multiple countries. And it is a two step process:

The *first* step is to create and implement a solid litigation readiness and response plan. When litigation hits, the *second* step is to harvest and process the data. This article will outline some of the best practices for collecting, filtering, processing, reviewing and finally producing data for EU electronic discovery.

First, some basics:

## ***The first step: what should organizations be doing?***

In the US, the need for corporations to create and implement a solid litigation readiness plan is ever increasing due to both the sheer volume of litigation that corporations are facing and the costs associated with eDiscovery.

Outside the US though, this need may not necessarily be so acute. For example within the EU outside of the UK, any litigation which a corporation is involved in that is to be heard by the local courts involves no discovery. So, if there is no obligation to find and hand over documents, then why spend the cost of preparing for such an eventuality?

The exception to this though is when corporations are facing regulatory enquiries, whether these be under the Foreign Corrupt Practices Act, competition inquiries or other agencies.

Historically, many corporations based in Europe have taken the view to “self-insure” – i.e. spending money in preparing for an unlikely eventuality is not viable and if such an eventuality was to hit them, then to accept that the associated costs are part of doing business. This however is slowly starting to change as corporations are increasingly facing regulatory enquiries. So, European subsidiaries are having to adopt some of the processes and procedures being used in the US.

The real first step for any organization is to have a document retention policy (for instance, determining what documents should be retained, for how long and where these documents should be stored, etc). Their document retention policy should also include the procedures for systematic destruction of documents. They should also have procedures to monitor and enforce compliance with these policies.

The company then needs to establish a protocol for responding to requests for electronic documents. The protocol should encompass identifying potential sources for relevant information and preservation of this information. It should also address the methods for extracting the data, and identifying and reviewing relevant documents.

As part of this plan you need to choose whether you have the resources and wherewithal in-house to collect and process elements of the electronic discovery or whether you need a partner who can work with you in a highly collaborative approach to meet your needs, one which is locally based and who understands the local rules and regulations.

***The second step: harvesting and processing the data***

Now, how is this done within the EU? This is where the fun starts. The European Union’s Data Protection Directive prevents companies sending personal data outside of the EU except when the destination country has been pre-approved as having adequate data protection. Only a handful of countries – Argentina, Canada, Switzerland, Guernsey, the Isle of Man and Jersey – have qualified as having adequate protection.

Despite these European provisions to protect personal data and restrict the transfer and use of that data, U.S. courts have been largely unsympathetic to defendants facing these obstacles and have even sanctioned companies who have failed to comply with discovery requests that violated local and international data privacy laws.

All countries of the EU have their own data protection acts however over the last year there have been two key realizations: data is being collected wholesale and shipped to the US with total disregard to the individual country rules; and there needs to be a mechanism in place to ensure that court requests for documents can be met without compromising the fundamentals of the right to privacy of the individual. There has been a lot of discussion as to how these conflicting requirements (US courts versus the rights of the individual) are going to be resolved. There have been two recent announcements in this area:

On 1 September 2009, Germany made some important amendments to their Federal Data Protection Act (The BDSG). The relevant amendments are:

- data controllers who engage a third party to process data will be guilty of a regulatory offence punishable by a fine if the data processing agreement is incomplete in contravention of Section 11(2) of the BDSG (Section 43(1) No. 2b). These new guidelines are more stringent than was the case before – when even the old ones were regarded as draconian by a lot of data controllers; and
- The penalties for violation of the BDSG have also been increased from EUR 25,000 to EUR 50,000 per violation and from EUR 250,000 to EUR 300,000 for serious violations

On 19 August 2009, the French Data Protection Authority (CNIL) released a new “opinion” on the transfer of data from France to a country outside Europe. The Opinion is noteworthy for describing how personal data can be transferred from France to the United States pursuant to U.S. discovery proceedings. The Opinion stresses that it does not cover proceedings originating from U.S. governmental requests, such as requests by the Security Exchange Commission (SEC) or the Federal Trade Commission (FTC).

So, until there is clarity what can corporations do? There are 3 options:

**Option 1.** The first method is for the corporation to adopt Binding Corporate Rules (BCR). This involves a company submitting its data protection processes to a data protection watchdog and having them approved for use. Once in place a national data protection authority can block a transfer only in very specific circumstances,. So far, however only 5 companies have made use of BCRs in the UK: Accenture, Atmel, Koninklijke Philips Electronics, General Electric and Hyatt as the process is both lengthy and costly.

**Option 2.** A second method is to allow the transfer of data across borders under the “Safe Harbor” framework. In order to bridge the different approaches to privacy between the US and the EU and to provide a streamlined means to allow US organisations to operate in Europe, the US Department of Commerce and the EU Commission developed a “safe harbour” framework which was approved by the EU in 2000.

Although the primary aim of safe harbour was to enable those companies with European subsidiaries to operate as if there were no borders, a plethora of organisations have now sought safe harbour accreditation (including a number of vendors in the eDiscovery space). To comply with the principles, a company needs to gain certification and have its name registered on the database of safe harbour companies.

The applicability of Safe Harbor certifications to e-discovery has been called into question however because the certification specifically dictates 7 conditions which must be adhered to by companies holding data under safe harbor. Not all of this sit easily because there a commonly held believe that because a company has Safe Harbor. data can be collected wholesale from the EU and transferred to the US. Key clauses are:

- *An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or*

*complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure.*

*- An organization must offer individuals the opportunity to choose (opt out) whether their personal information is to be disclosed to a third party*

*- Where an organization wishes to transfer information to a third party it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles.*

*- Personal information must be relevant for the purposes for which it is to be used.*

*- Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.*

**Option 3.** A third method is to obtain a letter of request under the Hague Evidence Convention from a district court. The Hague Evidence Convention is a treaty that allows the transmission of evidence from one state to another under certain guidelines. Obtaining an approved letter of request permits the transfer and processing of data. However, this process can take 6-12 months, often rendering this solution inapplicable to e-discovery requests with strict court-appointed deadlines.

### **Concluding Points**

It is clear that the current approaches to cross-border e-discovery each have their challenges in light of the vague and perilous data privacy landscape. As a result, corporations are having to look at alternative ways of meeting the conflicting requirements of the courts and the EU rules.

The Sedona Conference's *Framework for Analysis of Cross-Border Discovery Conflicts* (August 2008) supports this best practice saying, "*Generally, local counsel in the country where the requested data is located should be consulted to determine whether consent from individual employees, Works Councils or other bodies is necessary before processing or transferring the data. Any processing needed to determine the relevance of the personal data should be done within the EU before any transfer.*"


In this new approach, the first step is to collect, process, search, cull-down, and review data in country. This dramatically reduces the size of the dataset, allowing local counsel to quickly remove irrelevant documents and focus on the relevant data and custodians involved.

Once the relevant documents have been identified, the local counsel can redact personal information before exporting only the relevant documents. Processing, searching, culling, and reviewing the data set in country will reduce the risks associated with cross-border e-discovery.

The challenge with conducting e-discovery in-country is that it is perceived to be very costly and time consuming, especially when the expertise has to be flown to Europe from the US. Therefore in order for e-discovery in-country to be a viable option, corporations need to work with service providers who have the capability either in-country or with the ability to rapidly set up a facility in-country. These service providers should be able to fulfill the following criteria:

- Be able to react quickly
- Be able to deploy software with a minimum time delay
- These solutions must provide advanced search and analysis capabilities that enable early case analysis, rapid cull-down, and quick review
- Finally, these systems must be able to work with any language or character set by being Unicode compliant.

Organizations facing these cross-border e-discovery challenges must ensure that their people and processes match the technologies being utilized and are appropriate in their specific legal environment. The best way to ensure this is to solicit local counsel in the country in which e-discovery is being conducted. Not only can they advise on the local data privacy requirements that exist in addition to those dictated by the EU's Data Protection Directive, but they can add unique insight when interpreting email and document data that often contains local colloquialisms and contexts. This can prove invaluable when culling irrelevant data, conducting searches, and performing early case assessments.



THE POSSE LIST

SERVING THE CONTRACT ATTORNEY INDUSTRY

MANAGER@THEPOSSELIST.COM  
WWW.THEPOSSELIST.COM

1776 I STREET NW  
SUITE 900  
WASHINGTON, DC 20006  
202.286.3038

For more on the issues surrounding the international aspects of ESI collection and production check this link: <http://sn.im/t5ms>