Collecting Data in the EU
A Few Things You Should Know Before You Jump in the Water

A Catalyst Article

By John Tredennick
CEO
Catalyst Repository Systems
Collecting Data in the EU

Wading the Waters of EU Data Collection

When I was a young litigation partner (say about twenty years ago), collecting discovery documents was easy. Opposing counsel would send over 20 or 30 requests for production. I would read through them to see which could be dismissed as overbroad or otherwise improper. I would then send the remainder to my client with a note asking him or her to round up whatever could be found and send it back to me or my paralegal.

A few weeks later my client would send over a box of paper documents. We would stamp numbers on them, make a copy of everything and call opposing counsel for the production. In turn, opposing counsel would speak with their clients and send requested documents to me. That was about it for document productions.

It isn’t that easy today. In the digital age, the volume of documents has gone up substantially and most documents are now in electronic form. Rather than a quick telephone call, collections have become a complicated technical process involving networks, hard drives and a multitude of other devices. To make matters worse, courts increasingly are imposing sanctions against lawyers and inside counsel if the collections aren’t done right. Qualcomm is a good recent example (see my earlier columns on this case), but it isn’t the first, nor will it be the last.

The problem is compounded if your client is a multi-national. What if your client has employees in London or Brussels or perhaps Munich? What if they have been exchanging emails and electronic files that are relevant to your case? Is collection just a matter of a phone call to the foreign office? Can I dispatch a technical person to Europe to retrieve hard drives and PST files?

The short answer is no. The rules for collecting data in other countries are different than in the U. S. and those differences are important. If you collect the wrong data in the EU or collect the right data the wrong way, the penalties could be more severe than monetary sanctions. You might end up in jail.

Here is a look at some of the issues you face collecting data in the European Union. Many of these considerations also apply to data collections in other areas and many countries are following the EU’s lead. So, my hope is that this primer

* Published in the February 2008 issue of Law Technology Today (ABA Press)
will be useful to you wherever your client has offices and keeps its email, electronic files and other data.

**Privacy in the European Union**

For starters, we need to recognize that personal privacy is considered a fundamental right in many countries, one treated more strictly than in the United States. Data that relates to a person is protected in the EU much more carefully than it might be protected in the U.S. As a result, things corporations routinely do with data in the U.S. can get them into trouble overseas.

For example, email on a corporate server in the U.S. is considered fair game for discovery collections. Because the email system is owned by the company, we reason that employees have no expectation of privacy in their communications. Not so in the EU. There, email containing personal information is considered personal and subject to privacy rights even when it resides on a corporate mail server. If you plan to collect and review it, you better follow proper collection protocols. If you don’t, you are at risk.

Likewise, just because the files are on a corporate laptop in the EU doesn’t mean they aren’t personal to that employee. To the contrary, they are deemed just as personal as if they were on a home computer. Grabbing files off that hard drive using a network collection device could run you afoul of privacy laws in the country where the laptop is found. Even if you are thousands of miles away.

The bottom line here is that in the U.S. we think of data maintained on corporate networks as “corporate” data. In the EU the rule is different. They think personal data is personal wherever it resides and subject it to pretty stringent protection.

**EU Directive 95/46/EC on the Processing of Personal Data and the Movement of Such Data**

This privacy business got kick started in 1995 when the European Council (and the European Parliament) issued a key directive on processing and protecting personal data. EU Council Data Protection Directive 95/46/EC (24 Oct. 1995) (which I will refer to as the “Directive” or “EC-95/46”).

Drawing on principles issued fifteen years earlier by the OECD (Organisation for Economic Cooperation and Development, of which the U.S. is a member), the Council declared the following:

- That personal privacy is a basic human right in the EU;
Collecting Data in the EU

- That collection and processing of personal data must be consistent with the right to personal privacy;
- That collection and processing of personal data must be for specific limited purposes;
- That personal data be kept secure; and
- That personal data must be stored in the EU or in other countries that honor the EU privacy regulations.

EC-95/46, Article 4(1).

The Council went on to direct that each member state (currently 27 countries in Europe and the U.K.) enact legislation enforcing these directives. In the decade that followed, all of the member states did, with each writing their own set of rules for collecting and processing data. They also set up 27 separate Data Protection Authorities to interpret and apply their Individual rules.

What is Personal Data?

The definition of personal data is broad. In short, if it tells you anything about a person, it is personal. Specifically, the Directive defines personal data as “any information relating to an identified or identifiable natural person…”

Going further, the Directive states:

An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity…EC-95/46, Article 2(a).

This suggests to me that anything with a name, phone number or email address could qualify as personal. Thus, all email is personal as would be most documents showing an author. I call that pretty broad.

It doesn’t stop with the most obvious personal data. Some regulators in the EU have suggested that something as cryptic as an IP address (the numeric address assigned to your computer on the Internet) constitutes personal information. There is a healthy debate in recent issues of the New York Times over whether Google and Yahoo are violating EU privacy rules by collecting IP addresses from people who go to their sites. See “Europe: Your IP Address is Personal,” New York Times, Technology Bits, February 26, 2008.
The theory is that if you combined the IP address with some other information you could obtain from the user’s Internet Service Provider, you might be able to identify the individual.

What is Processing?

The Directive is couched in terms of “processing” personal data. What constitutes processing? Once again, the definition is broad:

“processing of personal data” … shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise …EC-95/46, Article 2(b).

For our purposes, anything we do to collect and work with data constitutes “processing” under the Directive.

When Can I Process Personal Data?

The Directive is straightforward on this point. As a general rule, you can only process personal data when you have the “unambiguous consent” of the person who is the subject of the data. EC Directive 95/46/EC, Article 7 (a). There are limited exceptions to this rule for “necessities” which I will discuss later in this column but they are often construed narrowly.

So what is unambiguous consent? Unfortunately, the answer isn’t all that clear and it may depend on which country is involved. Remember that each country was directed to write its own legislation implementing this Directive and the rules and interpretations for each can vary.

In at least one instance, German authorities suggested that an employee’s consent would be carefully reviewed under the German Data Protection Act,

The validity of consent to commence such procedure would have to be linked, among other things, to the requirements of its voluntary nature and of informing [the data subject] of the collection, processing and use of the data. It is doubtful as to whether consent can be granted voluntarily in an employment relationship.
In an employment relationship, one cannot regularly assume that consent has been given freely due to the hierarchical relationship between the company and its employee.


If every authority followed that logic, corporate collections and processing might grind to a halt.

**Who has to Consent?**

At a minimum, the Directive requires the consent of the “affected party.” But who is that? Even if I get the consent of an email custodian, what does that mean? His or her email will be filled with records containing personal information about other people. By definition, email is a communication involving multiple parties. Do we need consent from everyone that is identified in the custodian’s email?

If so the problem becomes boundless if not outright impossible. There is no practical way to track down the thousands of people who might be identified in my email files and no likelihood that they would all consent to your collection efforts. Thus, the rule seems nonsensical if strictly enforced, at least to me.

At a minimum (and this is just my opinion), you should have a written document setting forth the custodian’s “unambiguous consent” signed by the subject with a witness. The document should state simply and clearly (in the subject’s language of course) the following:

- Why the company needs this data;
- How it will be processed;
- Where the data will reside;
- What will be done with the data; and
- What measures will be taken to keep personal data secure.

Keep these documents in your files for safekeeping. You or your lawyers might need them years later when a problem arises.
What If I Can’t Get Consent?

The Directive provides several exceptions to the consent rule for “necessities.” What you need to know is that they are subject to interpretation by each Data Protection Authority and sparingly allowed according to most reports:

1. Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

2. Processing is necessary in order to protect the vital interests of the data subject.

3. Processing is necessary for compliance with a legal obligation to which the controller (company) is subject.

4. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (company) or in a third party to whom the data are disclosed.

5. Processing is necessary for the purposes of the legitimate interests pursued by the controller (company) or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests … of the data subject…EC-95/46 Article 7.

The first two exceptions related to the needs of the data subject and wouldn’t seem to apply to a corporation involved in litigation or regulatory proceedings. Items 4 and 5 are couched in terms of public and other legitimate interests which also would seem not to apply or would certainly require the exercise of discretion. That leaves item 3, which relates to legal obligations of the controller.

Given that most discovery is mandated by court order, it seems easy to make the argument that collection and processing is necessary to comply with a legal obligation. Unfortunately, EU authorities have taken the position that legal obligations only refer to obligations imposed by EU authorities and do not include a U.S. court.

Data Protection Working Party, Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime, at 7-8,
Collecting Data in the EU

In contrast, discovery sought under an international treaty involving the member country might be considered a legal obligation sufficient to invoke the exception.

However, you slice it, you are at risk collecting documents without individual consent by the affected individuals. And, in classic Catch 22 fashion, that consent may be impossible to obtain. Believe me, I am not making this up.

**Do I Have to Notify Anyone Before I Start the Collection?**

The short answer is maybe. The Directive provides for advance notification to data protection authorities in member countries before collection activities take place. EC-95/46, Article 18(1). The Directive also leaves room for exceptions and for simplified notification procedures.

Because each country has written its own rules, the answer will differ from country to country. For example, England takes the position that notification is not required in advance. However, if it is later found that you aren’t following proper procedures, you may find yourself in trouble. Other countries are far more strict. You should consult local counsel before you start collection efforts and make sure he/she is prepared to defend you if necessary.

**Assuming I Have the Data, Where Can I Keep It?**

Assuming you have collected data in accordance with the rules, the next question is where can you keep it? The safe answer is within the EU.

One of the central purposes of Directive 95/46/EC was to regulate the safe transfer of personal data among the member countries. As stated throughout the preamble, the Directive was designed, in part, to allow for the “free movement” of personal data within the member states and to remove any obstacles to the flow of personal data among them (e.g. Directive Title and Preamble sections 8 & 9). Thus, so long as the regulations of the individual member countries are followed, data can be transferred from one EU country to another without much worry.

This isn’t practical or cost effective in many instances. If the litigation or regulatory action is pending in the U.S. it is likely that the legal team is here too. Sending the team over on a European holiday to view data is not usually the best way to use your litigation budget. And, producing data to your opponent that has to stay in the EU might not be well received either.

Fortunately, the Directive includes provisions allowing for data to move beyond EU borders to other countries so long as one of the following requirements is met:
Collecting Data in the EU

- The receiving country has adopted laws that, in the opinion of the European Commission, provide “adequate protection” for personal data;

- The company exporting the data takes steps to satisfy local data protection authorities that the data will be adequately protected outside the EU; or

- One of several limited exceptions applies.

How Do We Determine Which Countries Offer An Adequate Level Of Protection?

The Directive doesn’t provide a final answer on that question. Rather, it authorized the creation of a Working Party comprised of representatives from the member countries to make such determinations. Over the years, the Working Party has declared that a number of countries including Canada and Switzerland, provide adequate safeguards for the protection of personal data.

What about the U.S.?

Because we do not have the kind of overarching privacy regulations typical in the E.U., the Data Protection Committee was loathe to declare the U.S. as having adequate safeguards to hold E.U. data. Naturally this caused quite a bit of consternation leading to negotiations between the U.S. government and EU authorities. Out of these negotiations came the “Safe Harbor” program that was to be administered by the U.S. Department of Commerce. The notion was, if a U.S. company complied with the Safe Harbor provisions, it could process and hold EU data just as if it was in the EU.

What is the Safe Harbor Program?

The U.S. Safe Harbor program is largely self-administered, which causes consternation for some. Companies and vendors that wish to participate in the Safe Harbor can register with the Department of Commerce on its website at http://www.export.gov/safeharbor/.

The requirements are relatively simple:

- The organization must register with the Department of Commerce to participate in the Safe Harbor program.
Collecting Data in the EU

- The organization must have a privacy policy in place that provides adequate safeguards for the protection of personal data including limitations on forwarding or otherwise sharing that data with others.

- The organization must provide a means of recourse to individuals claiming privacy violations both through the company and through public dispute resolution.

- If collecting personal data, the organization must agree to comply with EU data protection authorities and particularly agree not to forward personal data to others.

- The organization must publicly declare its participation in the Safe Harbor program and make its privacy and recourse provisions public.

Companies can apply online with the Department of Commerce and there is no formal audit process to ensure compliance. However, a company is subject to action by the FTC and other regulatory authorities if it misrepresents its status or doesn’t comply with Safe Harbor requirements.

When a company is accepted into the Safe Harbor program, it will be added to a public list of Safe Harbor companies maintained by the Department of Commerce on its web site.

Is a Safe Harbor Company Safe?

If you listen to some of the speakers at recent legal conferences, the answer is no. Indeed, one person recently labeled the Safe Harbor program as an oxymoron. According to the speaker, the program was neither “safe” nor a “harbor.”

If you follow that view, you would conclude that EU data needs to stay in the EU, despite the Safe Harbor provisions. With due respect, I think it is wrong. Keeping EU data with a Safe Harbor organization in the U.S. seems to be every bit as safe as keeping that data with an organization in the EU.

The Safe Harbor program was negotiated with the Commission of the European Union Communities. In July 2000, the Commission expressly declared that the Safe Harbor program complies with EU requirements. (Commission decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequacy of the protection provided by the
Collecting Data in the EU


The decision was binding on all of the member states who were directed to implement conforming legislation to make it effective.

In 2002, the EU Data Protection Council reviewed the implementation of the Safe Harbor program. It concluded that the program was working well on both sides of the Atlantic and that the privacy objectives were being met.


Tribunals in EU member countries have also recognized that the Safe Harbor program is safe, e.g. Data Protection Working Party, Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime, at 7-17, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp117_en.pdf

What Alternatives are there to Safe Harbor?

If the company receiving EU data (often the parent company) does not want to participate in, or use a vendor in, the Safe Harbor program there is an alternative. The company can enter into a data protection agreement with its EU subsidiary providing for adequate protection of the data. Fortunately, the European Commission has approved two sets of “model clauses” that can be used for this purpose. These agreements are sometimes called “transborder data flow agreements.”

Reportedly the EU is working on a third option called “Binding Corporate Rules” that can be adopted across a corporate enterprise to provide legally-binding protections for personal data that is transferred outside the EU. See Kate Boschee, International Data Protection Law Restrictions On International Transfers Of Personal Data, available at http://www.acc.com/chapters/program/dallas/dataprotect.pdf.
Collecting Data in the EU

Conclusion

Nigel Murray of London-based Trilantic reports that a data manager of a company in Finland was jailed for six months for not putting adequate controls in place to protect employee data. That’s JAILED FOR SIX MONTHS! He didn’t say whether it was the winter months, when it is cold and dark anyway, but either way that’s sleeping on a jailhouse cot and eating jailhouse food. That strikes me as pretty serious business even if the rooms are heated.

When I was collecting documents in my litigation practice, I never thought much about going to jail for doing it wrong. Now, I don’t mean to suggest you would be at risk of going to the hoosegow either. But I would certainly take care before starting a collection effort in the EU. And I would have my lawyer with me every step of the way.

About the Author

John Tredennick is a nationally-known trial lawyer and was a longtime litigation partner at Holland & Hart. He published his first of four bestselling books on litigation technology for the American Bar Association in 1990. An avid writer with scores of legal technology articles in print, Mr. Tredennick is also an accomplished and frequently requested speaker with both domestic and international expertise on litigation technology.

In 2000 Mr. Tredennick founded Catalyst Repository Systems, a document repository company that helps law firms, corporations, and governmental agencies manage evidence, people, and expectations for complex legal matters. Currently he serves as both Chairman of the Board and CEO and is responsible for Catalyst's overall direction, voice and vision.

Resources

Department of Commerce Safe Harbor Program
http://www.export.gov/safeharbor/

European Commission Web site on Data Protection

EU Home Page
http://europa.eu/index_en.htm

OECD Home Page
http://www.oecd.org/home/
EU Commission Decision on the Adequacy of the Safe Harbor Program

Data Protection Working Party, Opinion 1/2006 on the application of EU data protection rules to internal whistle blowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime, at 7-8,

Decision on Whistle Blowing Guidelines from the German Data Protection Agency,

International Privacy Organization
http://www.privacy.org/

The Asia-Pacific Economic Cooperation organization has released a similar privacy framework for consideration and implementation by member countries.
http://www.nacpec.org/docs/APEC_Privacy_Framework.pdf

The Trilantic Web site provides a wealth of information regarding the EU privacy laws along with links to legislation for each EU country.
http://www.trilantic.co.uk/resources/EU%20Data%20Protection.html

Worth Reading


http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1197281078728

Kate, “International Data Protection Law: Restrictions on International Transfer of Personal Data,” 2005