

# Are your data exports from Europe legal?

Four ways to comply with EU privacy rules

Jay Cline

April 6, 2006 ([Computerworld](#))

U.S. multinational companies have been taking a harder look this year at ensuring that their flows of personal data out of Europe are compliant with the European Union's Directive on Data Protection. Why the concern? Some EU data-protection commissioners are stepping up enforcement of the directive, which can mean stalled projects, fines or even jail time for their unlucky corporate victims.

If your company has employees in Europe or collects information from Europeans (through the Web, for example), you may be their next target. So what are your options to get compliant and keep your projects and company out of trouble?

EU officials have provided us with several different options. Which one is right for your company depends on what kind of data flows you have. The following are the main options that chief privacy officers are using:

1. **Transborder data-flow agreements.** These are contracts using the [model clauses](#) created by the EU. They're signed by the European entity exporting the information and the non-European entity receiving it. For example, a transborder agreement can be a contract among affiliates of your company in Europe, the U.S. and the Asia-Pacific region. Meeting the terms of the model clauses will most likely entail conducting a gap assessment of the data-processing operations involved in the data exchange and resolving any gaps you find. This mechanism works best if your company only has a handful of types of data flows leaving the EU, and those data flows don't change significantly from year to year. If you have dozens of types of data flows or affiliates, however, maintaining dozens of these contracts probably isn't desirable.
2. **Safe Harbor membership.** This is the option I see more U.S. companies considering. Joining the U.S. Department of Commerce's

[Safe Harbor framework](#) entails adopting a new privacy policy based on the seven Safe Harbor principles, conducting a gap assessment of your compliance with the policy, closing the gaps you find and filling out the agency's two-page application. Joining the Safe Harbor is best if you have numerous or changing data flows between the EU and the U.S. But the Safe Harbor doesn't cover data flows from the EU to Asia or most of Latin America, either directly or through the U.S. Transborder agreements are your best, and perhaps only, option for those regions. By the way, U.S. financial institutions and telecommunications companies are ineligible for the Safe Harbor because they aren't regulated by the Federal Trade Commission.

3. **Binding corporate rules.** This is a new option that only a few companies have pursued and only a few more are seriously considering. Binding corporate rules are the most comprehensive solution, enabling your company to have one set of documentation that brings into compliance all of your data flows outside Europe. But it's not easy. This option requires all of the policy-revision and gap-resolution steps of the Safe Harbor process, plus obtaining approval from the data-protection commissioner of each EU country from whose citizens you're collecting data. Binding corporate rules are best if you have complex data flows leaving the EU for all parts of the world.
4. **Customer consent.** The EU also allows companies to export personal data with the consent of the customer. This route requires you to get customers to sign a form or click a box before you can send their data outside Europe. The EU doesn't allow consent as a sole compliance option for exports of existing employee data, however, because the EU regulators believe employees aren't in a position to say no to these requests. Why don't I see privacy leaders taking this route very often? Because it involves losing customers who don't want to give consent, a result few companies want to experiment with.

Occasionally, I see companies taking other options. Perhaps the most common approach is simply to accept the risk of doing nothing. This happens for two reasons: Either the company's general counsel isn't aware that it isn't in compliance with the EU directive, or the company figures EU authorities won't notice its data flows.

Other companies deduce that their data flows are exempt from the law under the directive's provision, allowing data transfers that are necessary for the performance of a contract with the customer. But the EU takes so narrow an interpretation of "necessary" that the provision applies to only a handful of situations.

To be safe, companies should consult an outside attorney who is very experienced in EU privacy law before moving forward on any of these options. The attorney should be experienced in obtaining approval from European authorities for data transfers.

But the chief privacy officers I've spoken with in the past month aren't very satisfied with any of these options. They see them as only partial solutions that position their corporations for compliance with European privacy laws, but not those of Canada, Australia and Japan.

What we all really need is an international Safe Harbor: one global set of privacy rules to which any company in the world can voluntarily sign up for. This would make it a lot more likely that companies all over the world would focus their attention on what it really takes to protect privacy and prevent identity theft.

Exporting EU personal data: Which compliance option is right for you?		
	PRO	CON
Transborder data-flow agreements	<ul style="list-style-type: none"><li>Can cover data flows from the EU to any country</li><li>Whole company doesn't have to become EU-compliant</li></ul>	<ul style="list-style-type: none"><li>Hard to administer if you have many types of data flows</li></ul>

<p><b>Safe Harbor membership</b></p>	<ul style="list-style-type: none"> <li>■ Easier to administer than multiple transborder data-flow agreements</li> <li>■ Recognizable seal of approval for your company</li> <li>■ Can serve as an internal rallying point for compliance</li> </ul>	<ul style="list-style-type: none"> <li>■ Only covers EU-U.S. data flows</li> <li>■ Puts your company under the jurisdiction of the Federal Trade Commission</li> </ul>
<p><b>Binding corporate rules</b></p>	<ul style="list-style-type: none"> <li>■ Can cover data flows from the EU to any country</li> <li>■ Easier to administer than multiple transborder data-flow agreements</li> </ul>	<ul style="list-style-type: none"> <li>■ Approval likely required from many EU countries</li> </ul>
<p><b>Customer consent</b></p>	<ul style="list-style-type: none"> <li>■ Easy to administer</li> </ul>	<ul style="list-style-type: none"> <li>■ May lose customers who don't want to give consent or want to withdraw consent</li> <li>■ Alone, doesn't cover transfers of employee data</li> </ul>