

Managing Privacy Enforcement Risks in Europe

by Christopher Kuner and Aaron P. Simpson

While the enforcement of Europe's data protection law (roughly speaking, the European equivalent of privacy laws in the United States) differs from enforcement efforts in the United States, the consequences of such violations are no less real and serious. In recent months, political pressures at both the national and EU levels have caused European national data protection authorities (DPAs), individuals, labor unions and works councils to step up the pace of enforcement to unprecedented levels.

Data protection enforcement in Europe is carried out not by the institutions of the European Union (such as the European Commission) but by the DPAs. The pace of enforcement is likely to increase even further, as the committee of EU data protection authorities (the "Article 29 Working Party") is set to announce soon that it will carry out cooperative, EU-wide audits covering specific business sectors for the first time in 2005. Among the most likely sectors that the Article 29 Working Party will audit in the first wave are direct marketing, insurance and financial services.

The Case Against Microsoft

Microsoft's recent data protection troubles in Spain exemplify the obstacles facing multinationals doing business in Europe. In 1999, Spanish DPA officials inspected Microsoft Iberica SRL and discovered that the company owned a database containing personal data of Spanish citizens that did not comply with Spanish data protection law. These Spanish citizens had accessed Microsoft services at www.microsoft.com and Microsoft initially hosted the database containing their information in the United States. Later, Microsoft transferred the personal data from the United States to Microsoft Iberica in Spain. Based on these actions, the Spanish DPA initiated an enforcement action against Microsoft Iberica for violation of Spanish legal restrictions on the transfer of personal data outside the European Union.

In defense of its data handling practices, Microsoft Iberica argued that U.S., not Spanish, data protection law applied, since Microsoft initially hosted the database in the United States. In addition, Microsoft argued that, for each data subject, it had obtained appropriate consent or contractual authority to process the information on its database. However, the Spanish DPA determined that Spanish data protection law governed, and that explicit consent from individuals prior to processing and transferring of their personal data was required. The DPA found that Microsoft violated this law by transferring private data to Microsoft Iberica about individuals who had refused to allow Microsoft to transfer their private data to third parties pursuant to the choice offered by Microsoft in its privacy policy. The DPA punished Microsoft for this violation by levying a 50 million peseta fine, which was later reduced to 10 million pesetas (approximately \$60,000).

A Good Scolding

Another difference between EU and U.S. enforcement is that along with formal enforcement actions carrying specific penalties, DPAs in Europe

may also publicly reprimand companies by issuing harsh statements about their business practices. These public rebukes can be just as costly to companies doing business in Europe as fines are, as European consumers pay closer attention to statements made by DPAs than those made by their counterparts in the United States.

Other times, enforcement takes the complete opposite route. Data protection enforcement in Europe often takes place behind the scenes, with decisions of the data protection authorities often going unpublished, and case decisions in European legal systems are usually anonymized so as not to contain the names of the parties. Many times, enforcement actions are taken in consultation with the companies affected and never become public.

For instance, the authors are aware of a major company in Germany that was ordered by DPAs to remove all cookies from its website, which required major changes to its online presence. Such action was never made public, but the effect was just as serious as if the company had been forced to pay a large fine.

Recent enlargement of the European Union has increased membership to 25 countries, all of which maintain their individual languages and legal systems. Within each of these member states, data protection enforcement efforts differ in striking ways from those commonplace in the United States, which is due primarily to contrasting legal systems. The class actions, damage awards and contingency fees common in the United States are replaced by fines, injunctions, criminal sanctions and reputational harm in Europe, where the media and political spotlight shines more brightly on data protection and privacy issues.

Moreover, many more enforcement actions take place behind the scenes in Europe than is the case in the United States, although the consequences can be just as serious. Companies accustomed to U.S. privacy and data protection enforcement thus face a far different legal climate in Europe, but companies active there can often reduce their legal risks by following a few rules.

The risks posed by European data protection law can be difficult for U.S. companies to cope with due to the differences in the legal systems and the framework of privacy law. However, while such risks cannot be totally eliminated, they can be reduced to an acceptable level if companies take a few basic steps:

- Ensure that all European operations are in compliance with the requirements of local data protection laws. This can mean notifying the processing of personal data to the data protection authorities, ensuring that proper consents and policies are in place for the processing of employee data, and taking steps to provide a legal basis for the transfer of personal data outside the European Union.
- Appoint a privacy officer with the responsibility for overseeing compliance with the company's European operations.
- Instruct and train employees in the importance of observing data protection law and putting procedures in place to deal with compliance risks and legal violations should they occur.
- Learn the enforcement attitudes and practices of the DPAs in that jurisdiction in order to help identify where the greatest enforcement risks may lie.

In the end, European data protection law is bound to appear strange and unfamiliar to U.S.-based companies, arising as it does from a totally different legal tradition. But the risks can be managed, if proper due diligence is ensured.



Christopher Kuner is partner at *Hunton & Williams* where he works as head of the *International Privacy and Information Management Business Practice Group* based in Brussels.
Aaron P. Simpson is a New York-based associate at *Hunton & Williams*.