THE PRIVACY ADVISOR
The Official Newsletter of the International Association of Privacy Professionals
iapp
November 2009 • Volume 9 • Number 10
Editor: Kirk J. Nahra, CIPP

EuroPriSe – the new European privacy certification

By Jarno J. Vanto

What began as a pilot project in 2007 is now up and running under the management of the data protection authority (DPA) of Schleswig-Holstein, Germany's northernmost state, in partnership with the DPAs of Madrid (Agencia de Protección de Datos de la Communidad de Madrid) and France (Commission Nationale de l'Informatique et de Libertés, or CNIL), among other entities. Backed by European Commission funding, the European Privacy Seal (the Seal) for IT-products and IT-based services lets companies doing business in the European Union (EU) demonstrate privacy compliance.

The Seal is valid throughout the EU and can be used in both consumer marketing and public procurement, as laws in some EU Member States require governmental authorities to prefer Seal-carrying products over non-certified products in public procurement.


Jarno J. Vanto

Certifiable products and services

Privacy seals can be awarded to an IT-product, which can be hardware, such as a firewall, or software, such as a database application. Seals can also be awarded to IT-based services, such as online banks, search engines, or data centers. For example, to date, seals have been awarded to Surfboard Holding's Ixquick's search engine, Banco Guipuzcoano's BGNet online banking service, and Microsoft's Software Protection Platform. To obtain the Seal, these products and services had to pass a two-step certification process. They were evaluated by certified legal and technical experts, first, who issued a findings report that was then validated by Schleswig-Holstein's DPA.

Currently there are approximately 20 ongoing certification processes.

*See, **EuroPriSe,** page 3*

E-Discovery in Asia/Pacific: litigation readiness for Asian companies

By Thomas Shaw, CIPP

This is the first article of a three-part series exploring litigation exposure and readiness for Asian companies. Part two of the series will explain how non-U.S. companies, particularly those based in the Asia/Pacific region, can analyze and deal with the risks of U.S. litigation exposure to pre-trial discovery data requests.


Thomas Shaw

Due to expansive rules on discovery, jury trials, and the size of damage awards, plaintiffs worldwide choose to bring their claims in U.S. courts. So it is important that non-U.S. companies consider their exposure to U.S. litigation. After an Asian corporation has determined their exposure to U.S. litigation, they must take steps to analyze their current readiness to deal with requests for pre-trial discovery. Because response to discovery requests under U.S. rules is time sensitive, respondents must have the ability to fully describe their responsive data within about 100 days of the initiation of a law-

*See, **E-discovery in Asia/Pacific,** page 4*

This Month

French data protection authority issues new guidelines

By Olivier Proust

Olivier Proust

Pursuant to the Article 29 Working Party's guidelines on pre-trial discovery for cross border civil litigation issued in February of this year, the French Data Protection Authority (CNIL) recently adopted similar guidelines for companies based in France that transfer personal data to the U.S. in the context of civil proceedings. These guidelines are generally in line with those of WP 29, although the CNIL does address pre-trial discovery in light of French rules of civil procedure. French civil procedure requirements apply regardless of data protection requirements.

First of all, the CNIL clearly states that any disclosure of information to a U.S. court by a French-based company must comply with the Hague Convention of March 19, 1970 on the taking of evidence abroad in civil or commercial matters. This convention states that "a judicial authority of a contracting State may request the competent authority of another contracting State, by means of a letter of request, to obtain evidence." A reserve clause, however, authorizes a contracting State to refuse to execute a letter of request issued for the purpose of obtaining pre-trial discovery of documents. In France, a letter of request must be filed with the Minister of Justice who forwards the letter to the competent prosecutor's office. The prosecutor then transmits the letter of request to a judge who must verify whether it is admissible under French law and, in particular, must reject the request if it poses a threat to State sovereignty or to national security. The letter of request must clearly specify the information requested that has a direct relation with pending litigation in the U.S.

If a company does not comply with the Hague Convention, it can be found in breach of the Act of July 27, 1968 on the disclosure of information to foreign natural and legal persons. This blocking statute prohibits the disclosure of any information of economical, commercial, industrial, financial, or technical nature as part of foreign legal proceedings, unless this disclosure complies with applicable treaties and laws. Any breach

*See, **CNIL e-discovery guidelines,** page 14*

CNIL e-discovery guidelines

continued from page 13

of this statute is punishable by six months of imprisonment and a €18,000 fine. On December 12, 2007 the French Court of Cassation upheld the decision of a court of appeal that had sentenced a French attorney to a €10,000 fine for disclosure of confidential information about an ongoing merger between two companies in breach of the Hague Convention.

Disclosure of documents and information in the context of pre-trial discovery also requires companies to comply with the French Data Protection Act of January 6, 1978. Failing to do so exposes them to heavy criminal sanctions (five years of imprisonment and a €300,000 fine). Companies must verify that they have registered their data processing activities with the CNIL and that these activities are carried out in compliance with the privacy and data protection principles. In this respect, companies are strongly encouraged to implement adequate policies and procedures that will enable them to respond to discovery requests in compliance with these principles. For example, companies should filter the information locally, possibly with the assistance of a third party, in order to select the information that is relevant to a particular case and to limit the scope of information disclosed. Companies are also encouraged to anonymize or pseudonymize personal data prior to disclosing the information, whenever the identity of an individual is not relevant to the case. If necessary, personal data may be kept until the end of the case, but should not be stored indefinitely in anticipation of a pre-trial discovery request. Companies are also required to implement adequate measures designed to guarantee the security and confidentiality of personal data. In this respect, they may choose to archive their data after the retention period has expired, as described in the CNIL's guidelines on electronic archiving.

Perhaps one of the most controversial issues remains the legal basis used to transfer personal data to the U.S. Article 68 of the French Data Protection Act states that "the data controller may not transfer personal data to a State that is not a member of the European Union if this State does not provide an adequate level of protection of individuals' privacy, liberties, and fundamental rights." In the context of pre-trial discovery, the CNIL distinguishes between data transfers from France to the U.S. and onward transfers from a database located in the U.S. to third parties. Regarding data transfers, a data controller may either rely on the "establishment, exercise, or defense of a legal claim" exception (see Article 69.3 of the French Data Protection Act) for a single and limited transfer of all the relevant information relating to a particular litigation, or must provide an adequate

safeguard (i.e., Safe Harbor, model clauses or binding corporate rules) for massive and frequent transfers of personal data to the U.S. When the data are stored in the U.S. (e.g., centralized HR database), an adequate safeguard must nevertheless be put in place to disclose personal data to a judicial authority (i.e., stipulative court order) or to one of the parties (i.e., agreement or letter of engagement to abide by the Safe Harbor principles). Companies that have self-certified to the Safe Harbor principles may disclose personal data to third parties in compliance with the notice and choice principles. Personal data may be disclosed to a third party acting as an agent only if that agent subscribes to the Safe Harbor principles or is subject to the EU Data Protection Directive or another adequacy finding. To this end, a company may enter into a written agreement with the third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles.

The CNIL's guidelines should help French-based companies better understand the legal requirements that apply to them when confronted with a discovery request. Companies may decide that now is the time to implement internal policies and procedures aimed at coordinating and structuring the disclosure of information to U.S. courts in compliance with applicable French law.

Olivier Proust is an associate in Hunton & William's Global Technology, Outsourcing, and Privacy group. His practice focuses on all aspects of French and international data protection compliance projects, including implementation of global data management strategies, data transfers, and local data protection compliance. Proust also frequently counsels clients on various aspects of technology law, including privacy and security, e-commerce, and consumer protection. He is a member of the Paris Bar and the Brussels Bar E-List.

2009 Privacy Innovation Awards

HP and IAPP recognize winners in Boston

Hewlett Packard and the International Association of Privacy Professionals announced the 2009 Privacy Innovation Award winners at the IAPP Privacy Dinner in Boston in September. Barclays Bank PLC, Graduate Management Admission Council (GMAC) and IBM Research and Stanford University received this year's awards, which recognize privacy leadership.

This year's Large Organization category winner, Barclays Bank PLC, was chosen from a field of entrants for its cross-company effort to emphasize privacy awareness, compliance, and cultural change.

The not-for-profit Graduate Management Admission Council (GMAC) won the 2009 award in the Small Organization category. Earlier this year, GMAC received authorization from the French data protection authority, the CNIL, to use biometric palm vein technology to authenticate test takers at French exams. GMAC received the award for its data protection efforts toward the biometric authentication program.

IBM Research and Stanford University received the 2009 Technology category award for work that led to a significant advancement in encryption. Together, the institutions solved the challenge of "homomorphic encryption," or privacy homomorphism, whereby computers can process encrypted data without the use of a decryption key. IBM research scientist Craig Gentry accepted the award. He thanked IBM and Stanford University, adding that it has been nice to be able to conduct research that turns out to be a "force for good.

Read more about Craig Gentry's homomorphic encryption breakthrough in the July 2009 issue of the Privacy Advisor.

Read more about the CNIL's authorization of GMAC's use of biometric palm vein technology during GMAT exams in France on page 10.

Craig Gentry of the IBM Thomas J. Watson Research Center holds the 2009 Privacy Innovation technology award.