New York Law Journal

SERVING THE BENCH AND BAR SINCE 1888

VOLUME 242—NO. 114 | $3.00 WWW.NYLJ.COM MONDAY, DECEMBER 14, 2009 An ALM Publication

©2009 ALM

OUTSIDE COUNSEL

Tension Between EU Data Protection Laws and U.S. Discovery Requests

BY DANIEL SCHIMMEL

As a result of an increase in U.S. lawsuits requiring the transfer of personal data from France to the United States, the French Data Protection Agency (the CNIL) published a recommendation in August 2009, which is designed to offer guidance on data transfers in connection with U.S. civil discovery proceedings.[1] The CNIL's recommendation expands on the guidelines adopted by the body of European data protection agencies (the Article 29 Data Protection Working Party) in February 2009.[2]

EU member states increasingly enforce their data protection laws. For instance, in 2008, the Spanish data protection agency imposed fines amounting in total to €22.6 million. In France and other EU countries, companies are under pressure to comply with U.S. discovery requests, which frequently call for the production of personal data about employees, clients, or customers. The CNIL's recommendation reflects a tension between a company's obligation to respond to U.S. discovery requests and its obligation to comply with EU data protection laws. Because data protection laws pursue a legitimate interest and are increasingly enforced in Europe, courts and litigants in the U.S. should take them into account when ordering discovery abroad.

The CNIL's Recommendation

The CNIL acknowledges that the parties to a U.S. lawsuit have a legitimate need for documents, and that European and French data protection laws do not prohibit the transfer of personal data to the U.S. for litigation purposes. Such transfers, however, should be subject to certain requirements to comply with data protection laws. The CNIL's recommendation states, among other things, the following:

• Proportionality. A transfer of personal data to the U.S. must satisfy a "proportionality" requirement. According to the CNIL, to satisfy this requirement, the data processing must occur in the country where the data is located. Search terms should be used to focus on relevant data. The CNIL requests that a French company, when transferring "an important volume of data," consider redacting documents or use pseudonyms to prevent the production of personal data, if such data is not necessary or is only tangential to the case. Redacting personal data, however, may have the effect of rendering documents confusing. The litigants are therefore expected to confer about which data and documents are really necessary to the case.

Any personal data transferred to the U.S. should be limited to the identity, function, and contact information of the data subjects and should only involve data strictly necessary to the pending lawsuit. A "trusted third party," i.e., a person presumably having a sufficient level of independence or trustworthiness to ensure that the company has satisfied this proportionality requirement, should conduct a "serious verification." The CNIL does not define the volume of data that might call for redactions or identify the qualifications of the "trusted third party," although lawyers jointly retained by both sides or e-discovery professionals are likely candidates.

• Legitimacy. The processing of personal data must also be "legitimate." The CNIL states, among other things, that, to meet this "legitimacy" requirement, discovery must be conducted in compliance with the procedures of the Hague Evidence Convention.[3] In addition: (i) the data subject must have consented to the transfer of data, which, in countries such as France or Germany, is difficult to establish, especially with respect to employees; (ii) the entity that is the subject of the U.S. discovery request must also be under a legal obligation to comply under the laws of an EU member state; or (iii) this entity must have a legitimate interest in processing the data, such as the need to enforce or defend a legal right, and such interest must not be overridden by the interests for fundamental rights and freedoms of the data subjects.

• Procedures regarding the transfer of personal data to the US. The CNIL indicates that, where a person in France engages in a "single and non-massive transfer" of data to the US, which is necessary or legally required for the establishment, exercise, or defense of legal claims, the company responding to the U.S. discovery request does not need to request the CNIL's prior authorization, but should simply provide advance notice.

By contrast, "massive and repeated" transfers of data require the CNIL's authorization and are only lawful where (i) the recipient of personal data is an entity established in the U.S. that has subscribed to the Safe Harbor Scheme; (ii) the parties have adopted standard contract clauses issued by the European Commission; or (iii) the recipient has a set of strict and binding corporate rules in place providing an adequate level of protection of personal data. The CNIL does not provide guidance regarding the volume

DANIEL SCHIMMEL, a partner at Kelley Drye & Warren, focuses on international arbitration, transnational litigation, and international corruption investigations. Melissa E. Byroade, a litigation associate at the firm, contributed to this article.

of data that would trigger the need for CNIL authorization.

Stringent sanctions are imposed for violating French data protection laws. Because of this potential hardship, U.S. courts and litigants should become familiar with French data protection laws and the CNIL's recommendation. The CNIL can impose administrative fines amounting to 5 percent of the company's gross revenue, capped for now at €300,000, but a proposed bill submitted to the French Senate in November 2009 would increase this cap to €600,000. In 2006, the CNIL imposed a €30,000 fine on the French subsidiary of a U.S. corporation in connection with the transfer of personal data to the U.S. in violation of French data protection laws. Since 2005, the CNIL has imposed in excess of €520,000 in fines. In 2008, the CNIL searched the files of 218 companies; in 2003, only fifteen companies were searched.

In addition, processing personal data in breach of French data protection laws constitutes a criminal violation punished by five years' imprisonment and a fine of €300,000, which may be multiplied five times for companies (i.e., €1.5 million).[4]

More important, under French law, individual employees and unions have standing to initiate a criminal action for violation of the French data protection laws, which increases the likelihood of criminal actions. The ability of disgruntled employees or unions to do so makes it difficult for French companies to insulate themselves from criminal actions. Employees and unions can also seek a preliminary injunction enjoining the company from processing personal data in connection with a U.S. lawsuit in violation of data protection laws. Although the CNIL's recommendation is not binding on the French courts, it may influence their decisions.

Legitimate Interests

In determining whether to compel production of documents located abroad from foreign third parties, courts in the U.S. Court of Appeals for the Second Circuit focus on the following factors articulated in Aerospatiale and in subsequent cases: (i) the importance of the documents to the litigation; (ii) the competing interests of the U.S. and the foreign nation; (iii) the hardship that would be imposed on the foreign party or witness by an order compelling discovery; (iv) the availability of alternative means of securing the information; and (v) the good or bad faith of the party resisting disclosure.[5]

Courts have held that foreign parties and witnesses have a legitimate interest in the non-disclosure of personal information as required in EU data protection laws. In In re: Vitamins Antitrust Litig., the court held that disclosure of materials protected under the German Federal Data Protection Act (the BDSG) could only occur upon a showing that (i) "the information at issue is 'necessary' to protect public interests and/or the interests of plaintiffs," and (ii) "the data subjects have no 'legitimate interest' in preventing disclosure."[6]

The court held that the German defendants could file a privacy log detailing the information allegedly protected from disclosure under the BDSG, and that plaintiffs would determine whether such information was "absolutely essential to their case and whether there is a way to amend the Protective Order to safeguard defendants from liability in the production of this information."[7] Other courts have adopted the same analysis and have distinguished data protection laws from blocking statutes.[8]

In analyzing the hardship imposed on the party or witness by an order compelling the requested discovery, courts have recognized that the penalties for violations of data protection laws are substantial. The legitimate interests pursued in data protection laws, and the substantial sanctions available, should weigh in favor of compliance with French data protection laws and the CNIL's recommendation when ordering discovery in France.

Further, the CNIL states that a data transfer will only be legitimate if the discovery request was made in compliance with the procedures of the Hague Evidence Convention. There is a common misunderstanding that conducting discovery in France pursuant to the Convention is less productive and more cumbersome than doing so under the Federal Rules.[9] A decision of the Paris Court of Appeal, dated Sept. 18, 2003, one example among many, demonstrates that a letter of request designed to target relevant information in France will likely be enforced promptly and result in the production of broad categories of documents.[10]

Other European Countries

Other European countries, such as Germany, also increasingly enforce their data protection laws. In Germany, breaches of data privacy laws have raised the public's awareness regarding these topics. On Oct. 16, 2009, Deutsche Bahn was fined €1,123,503.50 as a result of violations of German data protection laws.

Data transfers from Germany to the U.S. have been scrutinized. In 2006, a German company, litigant in a U.S. lawsuit, was asked to produce the e-mails of 160 employees. The Berlin Data Protection Agency recommended that the company anonymize all documents in Germany prior to their transfer to the U.S. and, following the review of these redacted documents, select the relevant ones for production in non-redacted form. The German company stated that this was not practicable and ultimately reached an agreement with the Berlin Data Protection Agency setting forth multiple steps to secure the employees' consent (including the retention of a trusted third party) and transfer data to the U.S. in compliance with German data protection laws.

Certain amendments to the BDSG have come into effect on Sept. 1, 2009. Among other things, they have increased the sanctions available for violations of the Act, up to €300,000 under certain circumstances. Some commentators have also argued that these amendments raise questions about the ability to transfer personal data to the U.S.

Other EU countries have recently imposed significant penalties for violations of data protection laws, including Greece (a €76 million fine) and Spain. Although these and the Deutsche Bahn fines did not result from the transfer of data in connection with a U.S. lawsuit, they demonstrate that European data protection laws are increasingly enforced.

Conclusion

The CNIL sets forth important principles that should not be ignored by U.S. courts and litigants. Significant questions remain as to how these broad recommendations will be enforced in practice. The CNIL's recommendation may also give teeth to the blocking statute. The CNIL must refer any violations of French laws to public prosecutors and would be required to do so upon learning of violations of the French blocking statute.[11]

Endnotes:

1. Délibération No. 2009-474.
2. Article 29 Data Protection Working Party, Working Document 1/2009 on pretrial discovery for cross border civil litigation, adopted on Feb. 11, 2009.
3. Hague Convention on Taking of Evidence Abroad in Civil or Commercial Matters, 1970, 23 U.S.T. 2555.
4. The criminal penalties set forth in the French blocking statute are more modest, up to a six-month jail sentence and an €18,000 fine.
5. See Societe Nationale Industrielle Aerospatiale v. U.S. District Court for the Southern District of Iowa, 482 U.S. 522 (1987); Minepeco, S.A. v. Conticommodity Svcs. Inc., 116 F.R.D. 517, 522-23 (SDNY 1987); Weiss v. NatWest, 242 F.R.D. 33, 42 (E.D.N.Y. 2007).
6. No. 99-197TFH, 2001 WL 1049433 (D.D.C. June 20, 2001), at 8.
7. Id. at 9.
8. See, e.g., Minipeco, 116 FRD at 524.
9. See D. Schimmel & E. Rosenfeld, New Respect for Hague Evidence Convention in Discovery, NYLJ May 8, 2008.
10. Cour d'appel de Paris, 1è civ (CA Paris), Sept. 18, 2003.
11. Art. 40, Code of Criminal Procedure.

Reprinted with permission from the December 14, 2009 edition of NEW YORK LAW JOURNAL. © 2009 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited. For information, contact 877-257-3382 or reprints@alm.com.