BNA International

World Data Protection Report

International Information for International Businesses

Monthly news and analysis of data protection and privacy issues from around the world

Volume 10, Number 3 March 2010

UNITED STATES

Court Demands Data From Overseas Despite Foreign Data Protection Law

By Andrew A. Nicely and Joseph R. Baker, Partners in the Washington office, and Tim Wybitul, Partner in the Frankfurt office, of Mayer Brown LLP. The authors may be contacted at anicely@mayerbrown.com, jbaker@mayerbrown.com, and twybitul@mayerbrown.com.

Many foreign countries have enacted privacy laws and "blocking" statutes that limit the disclosure of personal data and other information maintained within their borders. Violation of these statutes can result in fines, civil penalties and, in some countries, criminal sanctions.

Parties involved in U.S. litigation frequently find themselves in a quandary when they are directed to produce documents stored overseas that fall within the protection of a foreign privacy or blocking statute; U.S. courts have generally been unsympathetic to such parties, commonly ordering production of overseas documents notwithstanding the obstacle posed by foreign law. Continuing this trend, a federal district court in Utah recently ordered a litigant to disclose certain data maintained in Germany that the resisting party contended were exempt from disclosure under the German Data Protection Act (GDPA).

AccessData, a U.S. software developer, brought suit against its German reseller, Alste Technologies, to recover certain royalties due from the sale of one of its products. *See AccessData Corp. v. Alste Techn. Gmbh*, 2010 WL 318477 (D. Utah January 21, 2010). Alste argued that it should not have to pay because, although many copies of the software product had been sold, the product was defective and had generated scores of complaints from customers. In addition, Alste alleged in a counterclaim that it had not been paid for technical support services that it had provided under its contract with AccessData.

To explore Alste's contentions, AccessData issued interrogatories and document requests seeking information about the customer complaints Alste had received and the support services it claimed to have provided. Alste objected to the discovery requests, arguing that the disclosure of information about its customers "would be a huge breach of fundamental privacy laws in Germany" — specifically, the GDPA. Alste contended that the discovery could be obtained only through the procedures established in the Hague Convention on the Taking of Evidence Abroad.

Alste did not specify the applicable GDPA provisions. Nevertheless, the court examined the statute and observed that Part I, Section 4c permits the transfer of personal information to foreign countries — even those that do not have the same level of data protection — if the "subjects" of the personal data consent, or if "the transfer is necessary or legally required . . . for the establishment, exercise or defence of legal claims."

The court noted that Alste had not shown that it was unable to obtain the consent of its customers, nor had it attempted to explain why the disclosure was not appropriate in connection with the "establishment, exercise or defence of legal claims." Even if those burdens had been met, the court concluded, relying on *Societe Nationale Industrielle Aerospatiale v. United States District Court*, 482 U.S. 522, 544 (1987), that the court was empowered to compel the production of the data even if it would require Alste to violate the GDPA.

The district court's conclusion that the GDPA's "defense of legal claims" exemption permits the transfer

of personal data for U.S. litigation might be viewed as inconsistent with German and EU interpretive guidance regarding the GDPA and the parallel provisions of the EU Data Privacy Directive. Absent the consent of the data subjects, German and EU authorities have permitted the disclosure of protected data for use in domestic or foreign litigation only where the requesting party can demonstrate that the information is necessary for the prosecution or defense of a legal claim and that the party's need for the data outweighs the privacy interests of the data subjects.

Last year, the Article 29 Data Protection Working Party, made up of EU data protection authorities, observed that a litigant's need for access to protected data must be "weighed [against] the rights and freedoms of the data subject who has no direct involvement in the litigation process and whose involvement is by virtue of the fact that his personal data is held by one of the litigating parties and is deemed relevant to the issues in hand, *e.g.*, employees and customers." Even where disclosure is permitted, steps such as redaction and data filtering may be required prior to transfer in order to minimize the impact on privacy rights and ensure that the disclosure is proportionate to the need.

When confronted with a demand for the production of data covered by a foreign data privacy or blocking statute, litigants and non-parties should consult with data privacy counsel in the foreign jurisdiction. Doing so will ensure that the requirements of the foreign statute are fully explained to the U.S. court, that the necessary approvals are sought from the appropriate data privacy officials, and that the data are filtered and redacted in accordance with the statute.

  WDPR ISSN 1473-3579