Privacy & Security Law Report™

January 24, 2011

EU Data Protection

Comments on EC Data Directive Amendment Call for EU Harmonization, Rules Clarification

by Emma Portier Davis

BRUSSELS—There were no surprises in a sampling of submissions reviewed by BNA that were filed by the Jan. 15 deadline for public comments on the European Commission's outline of possible amendments to the 15-year-old European Union Data Protection Directive (95/46/EC).

Organizations submitting comments called for increased harmonization of the application of the Data Directive, clarification of how and when national laws apply, and an improved process for finding country privacy regimes adequate for international data transfers. In general, the comments called on the Commission to lighten the administrative burden of compliance with the Data Directive.

The submissions were obtained directly from organizations by BNA, as the Commission has not made them publicly available. The submissions also raised questions about how the Commission's plan to introduce a "right to be forgotten" would work in practice, the usefulness of data breach notification, and the introduction of "privacy by design."

The Commission Nov. 4, 2010 released an official communication outlining possible amendments to the Directive (9 PVLR 1527, 11/8/10). It suggested measures to strengthen individuals' data protection rights, enhance the single EU market by creating a level playing field for companies handling personal data, protect data transferred outside the European Union, and to more effectively enforce privacy and data security law.

Call for EU-Wide Harmonization

Contributors from a variety of organizations—large corporate entities such as Intel Corp., the Association for Competitive Technology (ACT), which represents small and medium-sized enterprises, and think-tanks—were in agreement that harmonization is needed across Europe on the application of data protection law because the Data Directive is interpreted differently in many member states.

The European Privacy Association, a Brussels-based think-tank, said in its submission that legal harmonization "is key not only for data subjects but also for multinational companies established in several member states that (i) have to bear extra costs to cope with inconsistent rules on data protection and (ii) have no certainty of satisfying data protection rules and obligations."

According to ACT's comments, this is of particular concern for small and medium-sized enterprises that need a regime that is accessible in terms of legal and administrative costs and that allows them to develop services at an EU level. ACT noted that this issue was "particularly troublesome for the development of cloud computing services."

The American Chamber of Commerce to the European Union said in its submission that some definitions existing in the Data Directive may need clarification to provide for such harmonization, notably the concept of "personal data" and "consent." In the case of the latter, it called on the Commission to clarify that the validity of consent depends on the context.

Applicability of Member States' Laws

Many contributors also expressed concern about the ambiguity of Article 4 of the Data Directive, regarding the application of national law, the same subject as a Dec. 16, 2010 opinion of the Article 29 Working Party (10 PVLR 45, 1/10/11). The Art. 29 opinion sought to clarify when a particular member state's law would apply to a multinational company operating across borders in the European Union.

Intel's comments called for "an enhanced home country principle." This would allow for one data protection authority to be identified as the lead one for a company's dealings with the EU, determined by the location of that company's main establishment. Data subjects, it said, could still appeal to their national authority but mutual recognition would still allow for the other authority to take the lead.

The European Privacy Association charged that the present regime, under which national law applies in cases where a company carries out data processing within a particular member state's territory, "has resulted in significant compliance costs for such companies—that should not exist in the internal market—without generating significant benefit for data subjects."

Accountability Model Touted

The Centre for Information Policy Leadership at Hunton & Williams LLP (The Centre) proposed in its submission a new framework of Binding Global Codes to improve and streamline arrangements for international transfers. This would be based on an accountability principle that would encourage organizations to adopt measures to meet the objectives of the directive.

The American Chamber also asked the Commission to "explore the concept" of an accountability-based regime.

The European Privacy Association cited the accountability model with favor, noting that, like the lack of harmonization within Europe, the lack of easier means to transfer data across borders poses problems for the take-up of cloud computing.

"The cloud computing environment is a clear example of a sector in which the current legal means for transferring personal data outside of the EEA (European Economic Area) falls short," it said.

Right to Be Forgotten

Several contributors questioned the Commission's plan to introduce a "right to be forgotten" principle, which would give online users more control over how and where their data is retained. For example, such a principle could give users the right to permanently delete their profiles from social networking sites.

The Centre said it was skeptical about a simple right to be forgotten. "If this means more than the existing rights of erasure and blocking, it would come close to rewriting history," it said. The Centre said that this flew in the face of freedom of speech and press.

The Centre concluded that "any right to oblivion should not extend beyond personal data which is readily accessible in the ordinary course of business."

The American Chamber agreed, saying that the data control and retention powers ascribed to the right to be forgotten principle were already enshrined in the Data Directive.

"These provisions may not yet have lived up to expectations due to implementation and enforcement failures, but AmCham EU does not believe that this justifies the introduction of a 'right to be forgotten,' which inherently carries much wider ethical and philosophical connotations."

Breach Notice Fatigue

Several contributors warned that mandatory data breach notification requirements would lead to so-called "breach fatigue," which occurs when individuals have received repeated notices of data breaches.

The American Chamber said that if the requirements for breach notification is too broad it will be burdensome for businesses, and the notices will be confusing for or ignored by citizens. The group recommended that the European Union set a specific threshold for when notification of breaches is required according to the risk of harm to the individual whose personal data was breached.

ACT emphasized that data breach notifications could impose an unnecessary financial burden on small and medium-sized enterprises (SMEs) and also called for a breach notice risk of harm threshold "to avoid discouraging SMEs from developing innovative solutions and services."

No Mandatory Privacy by Design

Most of the contributions cautioned that privacy by design, which calls for building in privacy protections at the earliest design stages for products, services, and policies, should not be prescriptive.

The American Chamber went so far as to allege that "all legitimate businesses" already have privacy by design processes in place. It suggested that privacy by design be implemented via training programs for workers and policymakers. "It should not take the form of design mandate or technology preferences," the American Chamber cautioned.

Commission officials, who said the results of the consultation would be used to inform them in the drafting of formal legislation, have predicted that legislative proposals to amend the Directive are not expected before June 2011 (9 PVLR 1305, 9/20/10).

Any amendments to the Directive would be subject to approval by the European Parliament and EU member states.