THE PRIVACY ADVISOR
The Official Newsletter of the International Association of Privacy Professionals
iapp
Editor, Kirk J. Nahra, CIPP
May 2011 • Volume 11 • Number 4

More details emerge on the future of EU data breaches


By Jan Dhont and Katherine Woodcock

On April 5, 2011, the Article 29 Working Party adopted an opinion outlining its approach to data breaches (Opinion 13/2011 on the current EU personal data breach framework and recommendations for future policy developments). The Opinion examined the current status of the data breach framework within the European Union and highlighted points for cooperation and future policy developments on data breaches. These points include further action by the European Commission and the Working Party's desire to extend the ePrivacy Directive's data breach framework. What emerges from the opinion is the perception that the data breach requirements to be included in the amended Directive 95/46/EC (also referred to as the "Data Protection Directive") will be in line with the rules laid out in the ePrivacy Directive. Thus, the framework will ensure a harmonized regime and a coherent legislative approach by EU member states for data breaches in the EU.

Current Status
The first section of the opinion examines the current status of transposition of the ePrivacy Directive's mandatory personal data breach notification framework in EU member states. The framework contains certain key elements to be transposed, but the scope of the framework is limited to providers of publicly available e-communication services. The key elements are:

- the definition of a data breach
- legal thresholds for notification of authorities and affected individuals
- the content and timing of the notification
- the exemption for technological protections

Despite these key elements, the opinion identifies three areas where diverging approaches may emerge in different member states. These areas include: the scope of the application of the directive, the issuance of guidelines and the specific technological protection measures allowing the exemption from notification. The opinion acknowledges that the scope of application is likely to broaden beyond providers of publicly available e-

communications services, as even Recital 59 of the ePrivacy Directive calls on the commission to encourage data breach notifications throughout the EU "regardless of the industry or the type of data at issue."

Additionally, the issuance of guidelines by local authorities could diverge based on the different attitudes taken by the responsible authorities. Finally, since the ePrivacy Directive provides an exemption from the obligation to notify when data is rendered unintelligible to any person not authorized to access it, different levels of technological protection measures could emerge, as precise measures are not specified.

The Working Party's review was limited in scope, but included the current status of the directive's implementation (which is to be transposed by May 25, 2011). Most EU member states have draft texts, but many will not meet the transposition deadline. Nevertheless, according to the draft legislation, most member states closely follow the wording of the ePrivacy Directive and include the definitions and thresholds to notify relevant individuals in line with its wording. The specific areas where approaches by member states may diverge are subsequently singled out for harmonization either by cooperation between the national authorities or guidance by the commission. The Working Party notes that some of the EU member states' draft texts include various degrees of thresholds to inform individuals. Most member states have not expanded the scope of application beyond providers of electronic communication services, with the notable exceptions for Austria and Germany, who enacted data breach framework laws in the past. Half of the draft laws contemplate guidelines from the authorities, but questions remain as to which authority will issue such guidelines—the data protection authorities, the e-communications authority or both? Divergence in these areas could present obstacles for companies' compliance efforts and issues for individuals whose data is breached.

Future actions for cooperation and policy development

The opinion identifies areas for future actions for cooperation and policy developments to ease the burden for companies and enhance protections for individuals' data. With respect to cooperation, the Working Party states that it, together with the relevant national authorities, will act to raise awareness of security breach procedures and coordinate cross-border data breaches. The Working Party notes that some national authorities have experience with data breaches, while others are not familiar with the issue. Therefore, to ensure that all member states' national authorities have a uniform approach, the Working Party is committed to creating a subgroup to exchange views and knowledge on data breaches between the relevant authorities. The subgroup's initial matters will take the form of a knowledge center including 1) the circumstances where notifications to individuals would be necessary; 2) guidelines on the process and timing for notifications to individuals and authorities, and 3) evaluation tools to measure the effectiveness of technological protection measures.

Furthermore, the Working Party intends to create a platform and protocol to coordinate cross border data breaches. These would take into account the multi-jurisdictional aspects of data processing and differing establishments of data controllers. Prior to implementing such a platform and protocol, the Working Party wants to undertake a coordination exercise to analyze the applicable law and identify the competent authorities dealing with cross-border data breaches. This exercise would also be helpful in providing input relating to EU legislative policies, which the opinion further draws upon.

The opinion highlights areas of future policy development for the data breach framework, both for the ePrivacy Directive and in the context of the review of Directive 95/46/EC. The Working Party points out that, to ensure consistency in implementation of data breach framework, the commission is empowered by the ePrivacy Directive (Art. 4(5)) to adopt technical implementing measures concerning the circumstances, format and procedures on the information and notification requirements of the data breach framework. These measures are to be adopted following a consultation procedure with the European Data Protection Supervisor (EDPS), the

European Network and Information Security Agency and the Working Party and should also include the views of other stakeholders on the economic and technical aspects.

Finally, data breach requirements are being considered in the review of the Directive 95/46/EC. It is anticipated that the scope of application of this regime will be broadened to include all data controllers. Therefore, the new data breach framework would reach beyond the sector-specific application of the ePrivacy Directive (i.e. providers of publicly available e-communications services) to include all controllers of personal data. The Working Party points out that regardless of the scope of application, any new data breach rules should also need to be consistent with the language of the framework from the ePrivacy Directive to ensure harmonization throughout the EU.

Concluding recommendations

The opinion concludes with the Working Party's recommendations for future developments in the area of data breaches. The Working Party welcomes the extension of the scope of application of the data breach regime in the Directive 95/46/EC. However, it points out that while broadening the scope of application, the commission should stick to the key elements from the ePrivacy Directive. A new data breach regime should not be considered, as the stakeholders' (including the EDPS and the Working Party) views were considered when drafting the ePrivacy Directive's framework and any inconsistency would create conflicting obligations for companies and create an unlevel playing field.

Furthermore, the Working Party encourages a harmonized personal data breach framework taking into account the existing experiences of the member states with such laws. It notes that the e-Privacy Directive enables national authorities to issue guidance on the same aspects which the commission may regulate through its implementing measures. It recommends that the commission issues guidance on data breaches as soon as possible and encourage a survey of early practices. If the commission intervenes too late, it could result in divergence in national laws among member states. The Working Party's specific recommendations for the content of the commission's guidelines include: (i) the uniform circumstances where personal data breaches should be notified, as this would be especially helpful to data controllers active in multiple jurisdictions, (ii) the procedures in cases of data breach, (iii) a standard EU form to use when notifying, (iv) laying out the modalities for informing implicated individuals, (v) guidance on what information the data breach information providers are to retain, and (vi) what technological protection measures would allow notification exemptions.

The picture that emerges is that the Working Party would like to assure harmonization throughout the EU and create an EU data breach framework, including both the ePrivacy Directive and Directive 95/46/EC. Thus, businesses and individuals would have a single framework with only minimal discrepancies in the laws in the EU member states.

The full text of the opinion is available here.

Jan Dhont heads the privacy practice of Lorenz Brussels. He specializes in data protection and privacy, telecommunications, media and technology law. He can be reached at j.dhont@lorenz-law.com.

Katherine Woodcock is an attorney with Lorenz Brussels. She can be reached at k.woodcock@lorenz-law.com.