New Security Breach Notification Requirements Under Amended E-Privacy Directive

The Council of the European Union approved the so-called 'Telecom Reform Package' on October 26, 2009, providing for an overhaul of Directive 2002/58/EC on privacy and electronic communications (OJ L 201, 31.7.2002, p.37) ("E-Privacy Directive"). The new E-Privacy Directive contains an important number of amendments and it was published in the Official Journal of the European Union on December 18, 2009.

The goal of the amended E-Privacy Directive is to enhance the protection of individual privacy and personal data via ad hoc amendments that mainly aim at the encouragement of increased information security and enhanced enforcement powers to the competent national authorities of the member states (the "Authorities"). As amended, the E-Privacy Directive introduces an obligation to notify individuals and Authorities in instances of information security breaches. The scope of the E-Privacy Directive includes providers of electronic communication services such as telecom operators, mobile phone communication service providers, internet access providers, providers of the transmission of digital TV content (not the content providers), and other providers of electronic communication services. However, there are indications that this scope could extend beyond this sector mirroring the US notification requirements. This article will outline the notification regime for breaches of data, the new security obligations and the new enforcement mechanisms under the amended E-Privacy Directive.

I. Notification Requirements

The changes seek to encourage the development of data security via notification requirements in the occurrence of breaches of personal data. Requiring notification encourages accountability, drives investment in data security within provider entities and allows affected individuals to mitigate their damages. The ability to mitigate the risks associated with security breaches of personal data (e.g. identity fraud, humiliation, physical harm, etc.) is especially important, as it enables affected individuals to take measures to minimize damages. Also, notification requirements could drive competition in the field of data security technology for companies; allowing organizations to identify more effective methods of data protection and eliminate the less effective ones. This may further allow data controllers to assess the practicalities of individual security methods, driving the market for data security technology forward. Many companies perceive that such benefits of notification requirements come at their expense, since it is often embarrassing and tarnishes the public image of companies.

A. Who Must Notify?

The amendment provides a structure for notifying the competent authorities and individuals concerned when personal data has been compromised. Providers of electronic communication services are required to report security breaches. (Art. 4). There is a distinction between public versus private communication service providers; the E-Privacy Directive applies only to providers of public electronic communications

networks and services, i.e. telecom operators, mobile phone communication service providers, internet access providers, providers of the transmission of digital TV content (not the content providers), and other providers of electronic communication services that are offered to the public. (Art. 3). The European legislature explicitly stipulates that the directive "does not apply to closed user groups and corporate networks." (Recital 55).

It is important to note that the Article 29 Working Party ("WP") and the European Data Protection Supervisor ("EDPS") already encouraged the broad applicability of notification requirements, i.e. to private providers, due to the impact on citizens irrespective of the sector and the expansion of e-communications to process data. Thus, it is expected that industries that process important quantities of sensitive personal data may be subject to notification breach obligations in the future: The WP, in its opinion dated February 2009, expressed that notification requirements should also be extended to information society services provided by health care or financial institutions (e-health applications, e-banking, etc.). The current scope of the notification requirement would, according to the WP, reach a "very limited number of stakeholders" and "would significantly reduce the impact of personal data breach notifications as a means to protect individuals against risks". Furthermore, the European legislature encourages the expansion, as "interest of users in being notified is clearly not limited to the electronic communications sector, and therefore explicit, mandatory notification requirements applicable to all sectors should be introduced at Community level as a matter of priority." (Recital 59).

B. Requirements for Notification

The providers must give notice on two levels when a personal data breach has occurred. A personal data breach under the amended directive is defined as a "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of publicly available electronic communications services in the Community." (Art. 2(h)). The definition is very broad, since a small or initially innocent information security incident potentially constitutes a security breach. Upon breach, the provider must contact the Authorities without undue delay, in order to quickly address the breach and mitigate damages (e.g. economic loss and social harm). Additionally, if such a breach "is likely to adversely affect the personal data or privacy of a subscriber or individual", then the subscriber or individual should also be notified without undue delay. (Art. 4.3). Awareness of the breach enables the individuals to take necessary precautions and mitigate damages (e.g. cancel credit cards, change password, etc.). A breach adversely affects the data or privacy of a subscriber or individual where it could result in identity theft, fraud, physical harm, sign humiliation or damage to reputation. (Recital 61). However, the amendment is not clear as to who must make the assessment of the adverse effects on the individual – the Authorities or the provider.

Individuals do not need to be notified in some circumstances, specifically, when "the provider has demonstrated to the satisfaction of the competent national authority that it has implemented appropriate technological protection measures and that those measures were applied to the data concerned by the

security breach." These technological measures must render the data unintelligible to any person who is not authorized to access it. This applies to encrypted data and the exception provides that the Authorities decide if the providers have implemented sufficient protective measures and need not notify the relevant individuals or subscribers. Further, in cases where the providers have not notified the subscribers, the Authorities may require them to do so, if, after having considered the likely adverse affects, they deem it necessary. (Art. 4.3). It appears that consultations with the Authorities will increase exponentially and that further clarity will need to be provided by national legislators and Authorities.

C. Notice Contents and Procedures

The notice contents differ depending on the notice recipient, i.e. the Authorities or the individuals. The notice to the individual should "at least describe the nature of the personal data breach", provide a contact point where additional information can be acquired and should recommend mitigating measures to the possible adverse effects of the breach." Notification to the Authorities should, "in addition, describe the consequences of, and the measures proposed or taken by the provider to address" the breach. (Art. 4.3).

Further, the member states are encouraged to adopt measures delineating the circumstances, format and procedures for information and notification requirements, granting them increased powers to control the notification process. (See recitals 62-64). With respect the rules regarding format and procedures of notification, the Council suggests to take into account the circumstances of the breach, including whether or not the data was protected by adequate security measures. Providers must "maintain an inventory of personal data breaches" with the facts of the breach, effects of breach and action taken. (Art. 4.4). This is retained and allows for the Authorities to verify the providers' security obligations under the E-Privacy Directive. Audit may also take place to see if providers have complied with the inventory of breaches and the Authorities may also issue guidelines and instructions with respect to notification. (Art. 4.1a).

II. New Security Obligations

In addition to the notification requirements, the revised E-Privacy Directive implements new obligations for the security procedures of processing personal data. Additional language requires that providers must take appropriate measures to protect data being processed, including: ensuring such data is accessed only by authorized persons and that the stored and transmitted data is protected against theft, disclosure, or breach. (Art. 4.1a).

Finally, providers must implement a security policy, in addition to their existing requirement that they must take appropriate technical and organizational measures to safeguard the security of service and network security. (Art. 4.1a). Such measures should enable the providers "to identify vulnerabilities in the system." Furthermore, "monitoring and preventive, corrective and mitigating action should be regularly carried out." (See recitals 57 & 59). Such requirements and obligatory implementations contemplate that providers will keep up with the latest security technologies. Furthermore, providers' security procedures and corporate actions will evolve with these developments over time.

III. Empowerment of the Authorities

In order to facilitate better enforcement and compliance with the E-Privacy Directive, the Authorities are granted increased enforcement powers with respect to the security of processing (See Art. 4). The Council conceives that in order to promote the interest of citizens, the Authorities "should have the necessary means to perform their duties, including comprehensive and reliable data about security incidents that have led to the personal data of individuals being compromised." The Authorities should also monitor measures taken to mitigate damages and risks and disseminate best practices among the providers. As the providers must maintain an inventory of personal data breaches, this enables further analysis and evaluation by the Authorities. The strengthening of enforcement powers by national Authorities allows that the E-Privacy Directive is more resolutely enforced throughout the EU, although it does leave open the potential for varying national standards. Finally, new language allows for the member states to provide "penalties, including criminal sanctions, where appropriate, applicable to infringements of the national provisions adopted". These, of course, would have to be proportionate, but do express stricter entitlements under the reworked E-Privacy Directive.

On a whole, the Authorities are granted more power and enforcement mechanisms under the E-Privacy Directive. Further, notification requirements and security policies will force providers to keep up with current data security measures and burgeoning technologies. The expansion in scope of the notification requirements into other sectors is anticipated and encouraged by the EDPS and WP. This expansion will likely be observed during the implementation of the new directive by the member states in their national legal systems. Such implementation, combined with the possible expansion of notice requirements, could lead to laws that vary widely from member state to member state. This would make pan-European compliance difficult for businesses and it is hoped that the WP will timely provide for guidance to enhance a common standard.

Jan Dhont, Partner at Lorenz Brussels, j.dhont@lorenz-law.com
Katherine Woodcock, Associate at Lorenz Brussels, k.woodcock@lorenz-law.com