Notification of Personal Data Breaches under Luxembourg Law

Hervé Wolff

Data breach; Electronic communications; EU law; Luxembourg; Notification; Personal data; Service providers

Currently in Luxembourg there is no general obligation for data controllers to notify the authorities (or the customers) of data security breaches.

The EU proposal for a General Data Protection Regulation will introduce such a general data breach reporting obligation, with fines of up to €1 million, or up to 2 per cent of the annual worldwide turnover, whichever is greater, in the case of non-compliance.

However, there exists under Luxembourg law an obligation on electronic communications service providers only to notify the authorities of a personal data breach.

This narrower obligation was introduced by the law of 28 July 2011, which modifies the law of 30 May 2005 laying down specific provisions for the protection of persons with regard to the processing of personal data in the electronic communications sector (the Law of 2005).

Under art.2 of the Law of 2005, "personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the European Community.

In the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the Luxembourg data protection authority.[1]

EU Regulation 611/2013 dated 24 June 2013 provides for specific measures applicable to the notification of personal data breaches. In particular, the provider shall notify the breach to the competent data protection authority no later than 24 hours after detection, where feasible.

The provider must furthermore include in its notification to the data protection authority very precise information. This information includes the date and time of the incident; the circumstances of the personal data breach (e.g. loss, theft, copying); the nature and content of the personal data concerned; any technical and organisational measures applied (or to be applied) by the provider to the affected personal data; a summary of the incident that caused the data breach (including the physical location of the breach and the storage media involved); as well as the number of subscribers or individuals concerned.

Additionally, it is to be noted that the data protection authority has to provide to all providers established in the Member State concerned a secure electronic means for the notification of personal data breaches and information on the procedures for its access and use.

In Luxembourg, a form is available on the website of the data protection authority which has to be used by electronic communication service providers in the case of a personal data breach.

When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach. The data protection authority is allowed, in cases of repeat violations of the obligation, to notify a personal data breach, to deliver fines up to €50,000.

Such a sanction has, to the best of our knowledge, never been applied. Furthermore, according to the last annual report of the data protection authority,[2] there was no data breach notified to the authority.

* Avocat à la Cour; Partner with the Luxembourg law firm LG Avocats : hw@vocats.com.

[1] La Commission Nationale pour la Protection des Données.

[2] Commission Nationale pour la Protection des Données, *Annual Report* (2014).