# 11 DATA BREACH NOTIFICATION

## What is needed?

There are no 100% secure systems. This was demonstrated in December 2012 by the national railway operator in Belgium, SNCB/NMBS Europe, which leaked personal data of 1.4 million customers. In this database were personal data, including 5,682 email addresses from @ec.europa.eu (European Commission) and 1,668 European Parliament addresses. To date, the company has not notified any of the victims of the breach.

This incident shows quite clearly that the Commission proposals to introduce mandatory notifications to data protection authorities and to the victims of the breach should be supported. Existing laws in the US show that mandatory breach notifications are an effective tool to force companies and other organisations to quickly and comprehensively address breaches, as well as acting as an incentive for better security practices.

Moreover, supervisory authorities should maintain a public register of breaches. The safeguards against excessive notifications to victims and against excessive demands (companies are only required to act "where feasible") being made of the data controller are clear and reasonable. Any weakening appears entirely unnecessary.

**negative amendments**

Amendments have been tabled to weaken the obligation for companies and autorities to notify security breaches only when the breach is « likely to adversely affect » the privacy of citizens or if it is constitutes a « serious risk ». However, different controllers will define 'adversely' or 'serious' in different ways. In addition, it is naturally in a company's interest to underplay the impact of a breach on their customers for reputational and other reasons. These amendments are:

EPP : 1947, 1950, 1951, 1953, 1961, 2003 - ALDE : 1952, 1955, 1956, 1959, 1998, 2000 - ECR : 1997

Other amendments limit the breach notification to a narrow set of circumstances and suggest that processors should decide whether the breach needs to be notified or not to the data protection authority or the victim of the breach. Some amendments even go as far to delete the obligation to keep records of breaches.

Amendments: EPP : 1957 - ALDE : 1964, 1967, 1968, 1975

**positive amendments**

The introduction of a public register is a positive step since this can help to educate the public about IT security and provide added insight into trends regarding breaches. It is also beneficial, for legal certainty, to introduce the obligation to request the opinion of the European Data Protection Board before adopting implementing acts.

Amendments:

S&D : 1989, 1994, 1996, 2009, 2013 - GUE/NGL : 2004 - Greens/EFA : 198, 202



EUROPEAN DIGITAL RIGHTS