# Guidance on personal data security breaches: when obliged to notify and when exempt

**May 12, 2014**

**The Article 29 Working Party has published an opinion providing guidance on whether or not companies are required to notify data subjects in the event of a personal data breach. The opinion offers best practices for data controllers by analysing concrete examples of personal data breaches and illustrating precautionary measures that may prevent personal data breaches or mitigate any consequences.**

The Article 29 Working Party (Working Party) published an opinion on 25 March 2014 providing guidance on whether or not companies, being the data controller, are required to notify data subjects in the event of a security breach involving personal data. The Working Party describes what companies can do when implementing an IT system to avoid a personal data breach in the first place or, at least, what measures could have been implemented to exempt the company from the obligation to notify data subjects.

### Notification is already considered a best practice

Under the current EU Data Protection Directive, there is no generic explicit notification obligation for companies in the event of a security breach involving personal data as yet. So far, only telecom operators have an explicit obligation to notify competent supervisory authorities, and under certain circumstances even data subjects, under the EU e-Privacy Directive.

Based on the existing security breach notification obligation for telecom operators and the fact that there are two EU bills pending which will introduce a general security breach notifications for all companies processing personal data (the General Data Protection Regulation and the Draft Network & Information Security Directive), the Working Party considers that notifying the supervisory authorities and data subjects on a security breach already constitutes a best practice.

### Working Party provides guidance on when to notify

The Working Party provides a non-exhaustive list of examples of security breaches that adversely affect data subjects and therefore are not exempted from notification to data subjects. These include security breaches due to:

- the theft of laptops containing sensitive medical data of children
- unauthorised global access to a CRM system by a third party
- an envelope with credit card slips that is mistakenly thrown away instead of being destroyed
- a breach of a database containing passwords of users of a telecom operator
- the theft of laptops containing encrypted financial data
- a vulnerable web application of an internet service provider.

The Working Party analyses for all examples: (i) the potential consequences and adverse effects of the security breach, and (ii) what appropriate safeguards might have reduced the risks if implemented prior to the security breach.

### An example: vulnerable web application not exempted

An example of a security breach analysed in the opinion that is not exempted from notification to data subjects is the unauthorised access of personal data related to the customers of a life insurance broker due to a vulnerable web application where that personal data included names, addresses and completed medical questionnaires.

- The Working Party states that potential consequences and adverse effects of the security breach may include: (i) identity fraud or phishing, (ii) an emotional impact if the data subjects hide their diagnosed medical conditions, and (iii) an impact on the work and/or family environment.

### When are companies exempted from notification?

A company is not required to notify data subjects affected by a security breach when it demonstrates – to the satisfaction of a supervisory authority – that it has implemented and applied appropriate technological protection measures that render the personal data in the specific security breach unintelligible to any person who is not authorised to access it (such as encryption or anonymisation techniques). In such case, the security breach is unlikely to adversely affect the data subjects concerned and will therefore exempt the company from its obligation to notify data subjects.

### Recommendations

Companies are advised to:

- be proactive and take appropriate technical and organisational measures to avoid personal data breaches in the first place
- implement appropriate anonymisation and encryption measures to make use of pseudonyms and data unintelligible
- adopt and implement a response procedure for personal data breach to quickly and adequately deal with suspected personal data security breaches.