GDPR: a brief guide on data breach management

11 FEBRUARY 2019

Jacopo Liguori
SPECIAL COUNSEL | IT

CATEGORY:
ARTICLE

The several data breaches occurred in many sectors leads us to reflect on one of the most critical issues of the new privacy regulation (GDPR): the management of the obligation, for all companies, to notify a personal data breach and put in place a remediation plan. The matter at issue is actually very topical. Indeed, in the first six months of application of the new privacy law, 630 notifications to the Italian Privacy Authority have sprung up.

However, this phenomenon is not new within the Italian framework, since the obligation to serve a notification already existed for banks, telco, and companies that processed particular data (e.g. biometric data and health records).

More specifically, data breach concerns any abusive access, loss, or accidental alteration of personal data. In this context, Article 29 Working Party guidelines on data breach (WP250) contain numerous illustrative cases (see page 31 and following).

In the case of a breach, the company must notify the competent supervisory authority within 72 hours and, were the risk to be high, also the data subjects concerned.

Data breach is quite recurrent but does not necessarily have to be interpreted as a lack of compliance in the company that suffers it (even very sophisticated systems such as those of Google or Facebook can be breached).

Such breach cannot be avoided 100%, it is therefore essential to understand how to act if it occurs, minimizing the risk for data subjects, damages, loss of reputation and penalties. This applies both to structured multinationals and small businesses, as any company – regardless of its size – can process personal data, the breach of which may adversely affect the data subjects concerned.

First and foremost, there is the need to be technically equipped to be able to detect the breach in a timely manner (however, there are cases where detecting a cyber-attack breach may not be possible).

The use of own data protection tools can also help to avoid the risk (e.g. if there is a loss of encrypted data there may be no need to notify data subjects).

Nonetheless, it is also important to implement accurate and effective internal procedures that allow for immediate reactions and minimize the risks for the persons concerned by putting in place the so-called “remediation plans” (think of less structured companies in which, without a process to follow, it could be extremely hard to decide what the best way to proceed is).

Lastly, trained staff and privacy coordinators, as well as the Data Protection Officer (DPO) where present, are key figures as regards the management of the steps to be taken in the event of a breach. Moreover, in this respect, it should be recalled that data processors also play a pivotal role in the management of the process (sometimes they are the first to detect the breach, such as providers who manage databases). Precise contractual obligations of communication and indemnities for damages that could derive from the non-intervention must undoubtedly be taken into account during negotiations of data processing agreements.

Subsequently, a proper procedure and prepared staff allow for the best assessment as to whether the infringement does in fact constitute a data breach or there are high risks entailing an obligation to notify not only the privacy authority but also the data subject concerned and what measures and steps to take following the breach. The potential damage to the image of a company that notifies data subjects of a data breach that eventually proves to be risk-free can be lessened or, even a breach notified too late that has caused irreversible risks as a result of improper management can be mitigated.

As a matter of example, in a recent case it is helpful to point out that the data controller was certainly equipped with procedures and acted

promptly to manage the breach by notifying not only the privacy authority but also some of the data subjects for whom a high risk had been identified. However, once the notification was received, the authority imposed further measures on the data controller, considering it necessary to inform all interested data subjects.

The authority, referring specifically to the GDPR, considered that the personal data breach concerning the rest of the data subjects was also likely to represent a high risk to their rights and freedoms.

The infringement of those data, by ensuring a simple and prompt identification of the data subjects, made them easy targets for potential and rather foreseeable unlawful activities by third parties. Among those activities, current data subjects could have their identity stolen, misused or subject to phishing attacks.

On a final note, periodically carrying out vulnerability tests to strengthen systems and revisions of procedures to remedy any inefficiencies detected in the management of previous breaches should be remembered.

Authors

Jacopo Liguori

SPECIAL COUNSEL | MILAN

Intellectual Property and Technology

+39 02 8821 4204

jacopo.liguori@withersworldwide.com