

THE LEGAL MINEFIELD OF DATA PROTECTION

How Security Breach Legislation Affects Organisations In Europe

By Fran Howarth, Bloor Research

An escalation in the number of security breaches where sensitive information has been lost or stolen has resulted in regulations being brought in that mandate that those organisations that suffer such a breach must notify the individuals involved that their personal data could have been compromised. This can allow them to take steps to guard themselves against identity theft. But these regulations are by no means yet universally applied. Organisations need to be aware of their obligations in every country in which they do business—and be constantly on the lookout for new regulations being passed, or existing laws being extended to include security breach notification. They should then look at implementing technology controls specifically designed to automate the processes involved in achieving compliance with the regulations that they face.

1. Regulations Demand Better Control

The need to protect sensitive data such as customer lists, sales records, human resources information and financial details is enshrined in many regulations that organisations and government agencies face today. For example, the combination of the requirements of one of the most often cited regulations—Sarbanes-Oxley—mandate that executives must attest to having the proper internal controls in place to protect data against tampering, and must ensure the long-term retention, security, integrity and availability of data.

Some of the most recent regulations go one step further, requiring an organisation that has suffered a data breach involving personally identifiable information of living persons to publicly notify those affected that their information could have been compromised. At present, the majority of US states have enacted such legislation, as well as countries such as Japan, Hong Kong, Australia and New Zealand.



2. Data Protection In Europe

But where do organisations and governments stand in the EU when it comes to security breaches that compromise personal data? At an EU level, the primary instrument related to data protection is the EU Data Protection Directive of 1995. Whilst it is true that this directive does not contain any requirement for mandatory notification of a security breach, it is only a directive. That means that every member state of the EU has had to ratify its principles into their own national laws—and many of these are more prescriptive than the principles enshrined in the directive.

THE LEGAL MINEFIELD OF DATA PROTECTION

How Security Breach Legislation Affects Organisations In Europe

By Fran Howarth, Bloor Research

The seventh data protection principle of the 1995 EU directive requires that all data processing be undertaken in a secure environment, meaning that appropriate measures must be adopted to ensure that unauthorised processing does not occur and that data are not accidentally lost, stolen or destroyed.

The EU has been considering tightening rules concerning when organisations must notify the public of a security breach for some years, including strengthening existing legislation related to electronic privacy and data protection. The latest amendments to the ePrivacy Directive of the EU were made in May 2009, making notification mandatory for internet service providers and network operators should a breach such as theft or loss of a list of customer data occur.

Many say this does not go far enough. The European Data Protection Supervisor stated recently "Citizens will expect such a system to apply not only to their internet access providers, but also to their online banks and online pharmacies." And the European Network and Information Security Agency has recently recommended that the European Commission should introduce a security breach notification law. It states that such a law is necessary as many organisations are oblivious to their obligations as data controllers.

So does that mean that there are no specific laws that organisations, apart from those in the telecommunications sector, need to comply with in terms of breach notification? No—the situation is more complicated than that. In the light of the number of security breaches that have occurred recently—according to Data Breach DB, a clearing house for data breach information, more than 223 million records containing sensitive material have been compromised worldwide since 2005—many individual countries in Europe are using their existing data protection legislation or extending it to require organisations that suffer security breaches to alert their customers if there is a chance that a breach has put personal data at risk. This means that many are enforcing higher standards of data protection than those demanded by the 1995 EU data protection directive. This could potentially be a legal minefield for organisations that are not aware of the stance being taken in their own country—let alone for those that operate across borders.

3. The Cross Border Minefield

In the UK, the Information Commissioner's Office considers that organisations or agencies that have suffered data breaches through insufficient security, such as not using encryption for data on portable devices that are then lost or stolen, are in breach of the UK's Data Protection Act, which is its ratification of the 1995 EU Directive. It has taken enforcement action against nearly 100 organisations and government agencies that have suffered security breaches since 2007, forcing them to sign an

THE LEGAL MINEFIELD OF DATA PROTECTION

How Security Breach Legislation Affects Organisations In Europe

By Fran Howarth, Bloor Research

forcing them to sign an undertaking to ensure compliance with the seventh data protection principle.

Any business or government agency operating in Germany faces perhaps the most stringent data protection requirements in the EU. It has recently amended its Federal Data Protection Act, with changes coming into force as of July 2009, including the introduction of a new security breach notification requirement if the data loss is likely to have a serious impact on the rights of the individuals concerned. The new amendments require organisations to prepare incident response procedures and appoint an incident response team so that they can better respond to any security breaches that occur. It also introduces new powers for data protection authorities to order organisations to remediate compliance failures and increases the fines and sanctions that can be imposed for non-compliance.

Examples Of Sanctions Taken Against Organisations:

- The Nationwide Building Society of the UK: fined £980,000 in February 2007 following the theft of a laptop for failing to have effective systems and controls in place to manage information security risks. This was even though it had voluntarily informed customers that 11 million records had potentially been compromised.
- The insurer Norwich Union: fined after it had suffered a breach exposing details of 7 million people, allowing fraudsters to net £3.3 million by using details of 74 customers to cash in their policies. Such enforcement actions do not only hurt organisations financially, they will likely lead to customer attrition owing to the damage done to the brand.

4. The Cross Border Minefield

The implications for businesses and government agencies are clear—data protection is a serious issue and enforcement action is likely to be taken for any security breach that occurs. It is time for all organisations to review their data protection practices to ensure that they are in compliance with the laws of every jurisdiction in which they do business and every country where their customers reside.

To shield themselves from potential fines and reputational damage through the failure to adequately protect data, organisations and agencies must ensure that all of their employees meet the requirements for data protection enshrined in all the regulations that they face. Manually managing compliance efforts is a difficult task—especially given the number of regulations that require higher standards for managing electronic documents throughout their lifecycle and the need to report on compliance to government and regulatory authorities.