Rigorous audit

Whatever the impact of BREXIT on EU legislation, Roman Foeckl, CEO at CoSoSys explains why a 'by the book' audit is the essential first step to data compliance

Two years may seem like a long time, but for EU organisations, particularly those that deal with data pertaining to European citizens, it will pass quickly as they battle to implement the mandated procedures and tools that will ensure their compliance with the reformed GDPR. Actually, given the strict rules and the fact that very few companies already have clear guidelines and policies for data security, especially referring to data in the cloud, two years may not be enough. Then, there's the specific character of this form of regulation such as it being ambiguous or leaving space for interpretation: it's not going to be easy.

The highest success rate will be achieved by organisations that have a systematic approach based around the three steps of planning, execution and evaluation and usefully reinforced by some established policies. Whatever the case, chances will be maximised by starting immediately with an audit.

The reformed EU Data Protection regulation is like a tribute to individuals' private data, forcing companies to increase measures to protect data, to ensure its integrity and to respect an individual's right for data deletion. The audit will establish exactly what data is collected and processed, and to whom and where it is transferred, especially if it's leaving the EU. The importance of the audit is clear and the entire outcome of the process of becoming compliant depends on it.

There are several information audit management tools that can help with the audit, but they should always be accompanied by close supervision of key decision makers in the company, like CSOs, HR managers and other departmental managers that can advise on the business processes and the information flow.

Data Loss Prevention is also a key tool that helps the audit process. It offers detailed reports on data being transferred, by whom, through what applications or what removable devices. Research recently conducted at Infosecurity Europe revealed that USB devices still represent a big threat, with 61 per cent of respondents saying that they are not forced to use encrypted USB devices and 21 per cent admitting to the loss of a USB device containing sensitive data.

So you can see, knowing what data is being transferred to removable devices, on online services and applications, and the associated data, is vital for the audit and a first step in protecting data and complying with the revised data protection rules. DLP is the technology to help with this and since data controllers are responsible if data transferred outside of the EU is lost via a non-EU cloud provider, DLP will be even more important to detect sensitive data like personally identifiable information being transferred to online and cloud applications.

The three essential steps of audit are:

- Detect and define what sensitive information about employees, customers, and other stakeholders your organisation stores and processes. This step is crucial for later steps, when the actual implementation of the data security policies will take place.
- Check and review your privacy notices, especially in your direct marketing activities. Consent has to be expressed explicitly for any piece of information collected which should only be used for the mentioned purpose; also, data controllers must be able to prove valid consent.
- Extend the audit to the information security software and hardware your organisation uses.

The audit should reveal if the systems are updated with the latest security patches, if they cover all aspects included in the GDPR, if all threats vectors are somehow addressed, etc.

During the audit, all actions and data should be carefully documented. Next, the corrective and restrictive measures to support the new regulations and update the incident response plan are needed. It is only at this point that a solid foundation will be established for the future. NC