Working from home and secure emailing (1) (2/52/20)

Any company, state-owned or municipal institution or even sole trader that processes the personal data of EU/EEA residents enabling their identification is subject to the General Data Protection Regulation ("GDPR"). Its requirements extend to companies outside the EU/EEA offering goods or services to EU/EEA residents. This article explores ways of ensuring GDPR compliance when it comes to processing data in emails.

A company found to be in breach of the GDPR faces a fine of EUR 20 million or 4% of its total worldwide turnover in the previous financial year.

The first thing that springs to mind when it comes to processing data in corporate emails is GDPR requirements for marketing activities, including commercial messages, yet there are other equally important aspects, such as email encryption and security.

What companies are covered by GDPR requirements?

When a company gathers, keeps or otherwise processes personal data in EU/EEA countries, this processing is governed by the GDPR regardless of the company's location. Many companies will have to adjust their business model in order to meet GDPR requirements because every company is made up of people: staff, customers, and business partners.

The GDPR provides for integrated data protection and data protection by default, i.e. companies always have to consider the effect all new and existing goods and services have on data protection. GDPR article 5 lists processing principles a data controller has to follow. Encryption and pseudonymisation are only a few of the recommended technical measures aiming to minimise potential damage if a third party gains access to the company's emails.

Email encryption is a suitable method to maximise the protection of personal data available from emails. This helps the company show it has taken appropriate technical and organisational measures in data processing to ensure GDPR requirements are met and the data subject's rights protected. Though email encryption is not mandatory under the GDPR, each controller is required to take appropriate measures to ensure data processing is in line with the GDPR.

Email storage

To ensure personal data is kept no longer than necessary, the GDPR requires the controller to prescribe time limits for deletion or periodic review. The controller has to take all reasonable steps to correct or delete any data that is inaccurate. Deletion is a key part of data processing and data must be deleted to meet GDPR requirements. Deletion is one of six data protection principles. GDPR article 5(e) states that personal data can be kept no longer than necessary for the purposes it is processed for. Deletion is also one of a person's rights protected by GDPR article 17, the familiar right to be "forgotten." A data subject has the right to ask the controller to delete their personal data without undue delay, and the controller has to do so without undue delay. Of course, each request should be assessed on its merits and there are

exceptions when the controller (company) may refuse deletion (e.g. in the public interest). Barring reasonable exceptions, the controller is required to delete any personal data they no longer need or that has become useless for the purpose it was originally obtained for.

How can data deletion requirements be applied to emails? Many of us never delete our emails. There are many good reasons to keep them for some future use. We may have to review our emails sometime in dealings with our business partners, or our emails might contain some information necessary for pending litigation. Though these reasons for keeping data are very important, one thing to remember – the more data we keep the greater the company's liability will be if a data breach occurs. And the EU legislation provides for deletion of unnecessary personal data. The GDPR requires a company to periodically revise its email storage policy in order to minimise the amount of data stored in staff emails and to compile only the information that could be necessary for the purposes described above. The company must have documentation that balances its legitimate business interests with the data protection duties laid down by the GDPR.

From a technical viewpoint, deleting data available from emails can be a fairly straightforward process the company can automate to ensure its emails are deleted with a regularity it prescribes. Whatever policy on email storage and deletion the company adopts, this helps it mitigate GDPR non-compliance risks significantly.

(to be completed soon)