Working from home and secure emailing (2) 3/2/21

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 completes what we wrote on this topic last year.

Marketing activities and emailing commercial notifications

To comply with data processing principles laid down by GDPR article 5 companies have to ensure their processing is lawful, fair and transparent in relation to data subjects. A company can process personal data only if it follows all those principles. So companies have to be fair towards data subjects (individuals) and any type of processing has to be based on clear communication with them.

GDPR article 6 lists six legal grounds an organisation can have for processing (gathering, storing, using etc) personal data.

Under GDPR article 6(1)(a) a data subject has consented to having their personal data processed for one or more specific purposes. Consent has to be fairly obtained and based on the company's full and clear explanation of its intended processing:

- Consent has to be given freely and it has to be specific, informed, and unambiguous;
- The consent request has to be clearly separated from other matters and written in a clear and comprehensible language;
- The individual can revoke their consent at any time and the company has to ensure such revocation is carried out immediately unless there is a good reason why the company is unable to do so;
- Children under 13 can give consent only with permission from their parents;
- The company has to keep documentary evidence of consent.

Under GDPR article 6(1)(f) processing is necessary for legitimate interests the data controller or a third party pursues, so the company carries out processing according to its lawful interests. However, when it comes to using this legal basis we must remember that the data subject's fundamental rights and freedoms may override the company's lawful interests so this legal basis may prove to be inapplicable and processing therefore impossible.

An organisation pursuing its lawful interests can send commercial notifications to another organisation's email address without obtaining its prior consent but this must be done from a valid email address to which the addressee can send a request that communication be stopped. This procedure has to be followed also in emailing commercial notifications to individuals, and their contents have to meet the requirements of section 8 of the Latvian Information Society Services Act.

The GDPR does not ban the emailing of commercial notifications or the use of individuals' email addresses for marketing purposes. In the case of good marketing, however, the addressee will welcome more notifications to their inbox, for example, about the company's services. The GDPR clarifies the consent rules by requiring companies to seek an affirmative choice if they are to email commercial notifications. A company breaches the GDPR only if there is no way the consumer can unsubscribe from commercial notifications, or if the company ignores the consumer's choice or sends information to someone who has not consented to receiving it and has not used similar services before.

Email security

Under GDPR article 5(f) personal data has to be processed in a way that properly safeguards it, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Email encryption is one of the technical measures a company can take to ensure data processed in its emails is secure. Organisational measures have to do with corporate policies and procedures and the provision of training. Hackers use phishing emails to access a user's account or device through deception or malware. If the recipient clicks on or downloads an attachment, this action can give the attacker access to the recipient's device and often to other devices owned by the company and email users' accounts, so one careless employee can put large amounts of data at risk. If the company is unable to satisfy the regulator that appropriate technical and organisational measures are in place, the company may have to pay a hefty penalty for non-compliance with the GDPR, as well as having to compensate individuals (data subjects) for infringing their rights.

To mitigate the risk of breach, it is important for companies to educate their staff about email security and to adopt technical and organisational solutions that best protect personal data in order to minimise a potential penalty.