How to check compliance with GDPR (1) 1/32/20

The mass media have recently reported news of the largest fine in Latvia to date (EUR 150,000) being levied on an e-commerce company for breaches involving failure to comply with requirements of the General Data Protection Regulation ("GDPR"). Considering the company's circumstances, as cited by the National Data Office in its decision, this article explores requirements that must be met by any company processing personal data on its website to steer clear of the fine prescribed by the GDPR.

Provisions of the GDPR

The GDPR governs all companies offering goods or services to EU nationals and applies to any e-commerce company using the data of persons living in the EU. The GDPR covers all databases containing user information, such as credit card data and purchase data.

Under the GDPR, breaches (including the one in Latvia) attract fines of up to EUR 20 million or – in the case of the Latvian company – up to 4% of its worldwide turnover in the previous financial year.

Things to consider when processing user data on websites

Failure to comply with the GDPR may not only cause a large financial loss but also harm the company's reputation, reducing its ability to win business in the future.

A privacy statement on the website

A privacy statement is a public document that must describe how the company applies the principles of data protection. The GDPR requires a privacy statement to be concise, transparent and unambiguous, and it must use a simple language to ensure that any person visiting the company's website is informed in a comprehensible way about data processing done by the company.

The majority of large companies have probably put up a privacy statement on their websites, paying attention to the following aspects:

- Has the company updated its privacy statement since 2018 to ensure it corresponds to the present situation and covers all personal data collected from the moment a user visits the website?
- The privacy statement must clearly define the purposes for which the company uses personal data, e.g. marketing or accounting purposes;
- The privacy statement must clearly state the website user's rights relating to their personal data and how it is used;
- Each purpose of data processing needs a legal basis, about which the company must provide information to the user;
- The website must give information about who may process data and how the processing may be done;
- The user must have clear information about whether their personal data is processed on the basis of consent, law, or contract. It is important to note that the legal basis may vary according to the purpose of personal data processing, and this information must be clearly stated on the website.

Does the company receive consent from website visitors and existing customers before obtaining their data?

The GDPR aims to provide customers/users with complete control over the use of their data online, including e-commerce. Consent is a key element of data protection.

For example, an e-commerce company must have legitimate solutions for obtaining consent and for further data processing based on that consent. A privacy statement must provide all the required information about collecting, processing, storing and using customer/user data. When personal data is processed in forms, registration processes, emails and pop-up banners, the company must enable the user to give or withdraw consent to the use of their data.

Below are the main questions about personal data processing based on consent:

- Is consent the legal basis for obtaining personal data? Or is there a different legal basis for data processing?
- Does the procedure for obtaining the data subject's consent meet all the criteria relevant to e-commerce and the GDPR criteria?
- Is the company able to prepare information, e.g. for submission to the regulator, proving that the data collection and processing have a legal basis?
- Has the company documented all cases where it processes data on the basis of consent?
- Has the company revised its processes of obtaining consent? Does the company revise/update those processes regularly?
- Is it possible to stop the data processing and delete entries after receiving a request from the data subject?

(to be completed)