How to check compliance with GDPR (2) 1/33/20

This article completes what we wrote last week about the General Data Protection Regulation ("GDPR").

Disclosing customer/user personal data processing activities

Companies must prepare clear descriptions of their processes and purposes of data collection to explain why data is collected, processed and stored for a certain period. These processes include data categories, storage periods, and deletion checks. Companies should also describe security measures they take to protect personal data.

The GDPR grants eight rights to the person:

1. the right to be informed;
2. the right of access;
3. the right to rectification;
4. the right to erasure;
5. the right to restrict processing;
6. the right to portability of data;
7. the right to object to processing; and
8. the right related to automated decision-making, including profiling.

Acting on a breach of data protection

The possibility of data breaches is a good reason to revise existing data processing procedures, especially in e-commerce companies. The GDPR requires all companies to notify a supervisory authority of data protection breaches if criteria for the duty of notification are met. Reporting must be done within 72 hours after the company became aware of a breach. If the nature of the breach is likely to affect the person's rights, the incident must also be notified to the company's customer and/or website user. And every company must register data breaches regardless of their nature.

Below are the main questions to be answered about data protection:

- Does your company revise its IT systems and processes to prevent data breaches and to address related issues?
- Is your company aware that it has a high risk according to criteria for data protection breaches requiring your company to notify a supervisory authority?
- Does your company have a procedure in place for reporting data protection breaches that meets all GDPR requirements?
- Has your company set up an internal system for reporting potential data breaches?

A company trading outside the EU

Under EU data protection enactments, including the GDPR, personal data may be transferred only to third countries that guarantee a level of data protection consistent with the GDPR requirements for member states. Any third country to which personal data is transferred must maintain an appropriate level of data protection, and all companies, including e-commerce entities, must meet the GDPR requirements

regardless of their geographical location.

Conclusion

It is important for every company to understand that the GDPR applies to all personal data relating to an identified or identifiable person. This information includes personal data relating to the person's name, birth date, credit card details, bank transactions, social networking sites, and even photos, as well as a considerable amount of other data the company may acquire from the moment a customer/user visits the company's website for the first time. Also, any cookies the company uses and any customer/user IP addresses it obtains are personal data that may be processed only in line with the GDPR requirements.

It is important to note that the GDPR covers all companies that offer goods and/or services to EU nationals, i.e. any company, including an e-commerce entity, that uses the personal data of individuals living in the EU.