New Privacy Rules for European Union Will Apply to Companies Worldwide

A new regulation will apply to all European Union (EU) citizens and therefore to all companies in and outside the EU that process data of citizens of the EU, e.g. data related to the offering and selling of goods or services. In order to protect the privacy of EU citizens, the European Parliament adopted a General Data Protection Regulation on March 12, 2014, which is likely to become effective in 2017. This regulation will change the current privacy law and will have direct effect in the whole EU. As there will be severe fines for (repeated) breaches of the new regulation, it is very important that businesses take timely measures to comply with it. It is expected that the new European regulation will also have implications for privacy rules in, for instance, the United States, as many American businesses are active on the European market.

So what are the most important provisions of this regulation? The EU citizens will get new rights, for example the right to information and the right to be forgotten. On the other hand, companies which are working with personal data have to deal with new obligations, for instance: appointing a data protection officer, assessing the processing of data in their company and providing information to those concerned.

Fines

One important aspect of this regulation will be the introduction of new penalties including extremely severe sanctions for (repeated) breaches of privacy of EU citizens. At the moment, e.g. the Dutch Data Protection Agency (College bescherming persoonsgegevens) can impose a maximum fine of EUR 4,500. However, the new fines could be up to maximum of EUR 100,000,000 or 5 percent of the global annual turnover of a company, depending on which amount is higher. Fines are imposed for the following violations, for instance:

- Processing of personal data without consent or legal basis.
- Processing of personal data with regard to:
  - Racial or ethnic origin
  - Political opinions
  - Religious or philosophical beliefs
  - Trade union membership
  - Genetic information
  - Health
  - Sex life
  - Criminal convictions and related security measures
- Not taking appropriate technical and organizational measures to prevent data leaks, unauthorized access to and elimination of data.
- Not reporting data leaks in time, for instance, loss of a USB device or website hacking.

Reinier W.L. Russell

Reinier W.L. Russell is managing partner of the law firm of Russell Advocaten B.V. He is an experienced outside corporate counsel to both domestic and foreign businesses in the Netherlands. He deals with business formation and reorganization, corporate governance, insolvency law, employment issues, real estate issues and all aspects of e-commerce and contract law.

Russell Advocaten B.V.
Reimersbeek 2
1082 AG Amsterdam
Netherlands

Phone: +31 20 301 55 55
Fax: +31 20 301 56 78

reinier.russell@russell.nl
russell.nl

- Non-performance of data protection impact assessment upon processing data that involve special privacy risks, for instance regarding health.

Data Protection Officer

According to the regulation, the following businesses and organizations must appoint a data protection officer:

- Businesses with more than 250 employees
- Companies processing data of more than 5,000 persons within a period of 12 months
- Government authorities/public bodies

The data protection officer – also referred to as privacy officer – is an independent person who monitors the general quality of the data protection policy of an organization. The data protection officer will control whether the processing of data in a company is in accordance with the Data Protection Act. If the data protection officer detects irregularities, he must report them to the person in charge or to the company he was appointed by. In addition, the data protection officer is allowed to make recommendations. However, these recommendations have an advisory function only. Ultimately, it's up to the person in charge whether to follow the advice of the data protection officer or not. Appointing a data protection officer might imply that the national data protection agency will act reluctantly if the data protection officer performs his duties properly.

Data Leak Notification Requirement

A new data leak notification requirement will be introduced. This means that if a company has been affected by a data leak, it has to report it within 24 hours to the relevant authorities. There is a notification requirement in the event of a breach of an organizational security measures for data. Examples are: theft of password or client data, hacking or loss of data, for instance, if an employee has lost a USB device.

A data leak must be reported by the person in charge of data processing in a company, for instance the data protection officer. If a breach could lead to the risk of negative consequences for the protection of data, the responsible person needs to notify the relevant authorities and also all persons who are concerned in this matter.

A breach of data processing needs to be reported by the person in charge within 24 hours after noticing. If a breach of the data processing isn't reported within 24 hours, a specific explanation must be provided. An organization that doesn't report a violation completely or in a timely manner will risk incurring a severe fine. The amount of the fine will be determined based on the facts, as, for instance, prior breaches, the scope of the breach and whether it's a question of intent of gross negligence.

Right to be Forgotten

Pursuant to the new regulation, the consumer has the right that companies and institutions delete the data and that further spread of the data will not occur if:

- It is no longer required to store the processed personal data for the purpose they used to be collected or processed for;
- The person in question withdraws his/her consent, and/or when the period allowed for data storage has passed;
- The person in question lodges a complaint against the processing of personal data;
- The company or institution does not comply with the other provisions of the regulation.

The regulation requires not only to delete the data in question but also to prevent further spread of the data. Therefore, a company is obliged to inform third parties who process data provided by the company of the person in question's request to delete any link or copy of the personal data. It is wise to create a protocol for handling requests about information, modification or deletion of personal data according to the new regulation.

Conclusion

In view of the fact that the fines businesses can incur are a lot higher than before, it is really important that companies throughout the world are fully aware of the rights and obligations of EU citizens that arise out of the new regulation. It must be taken into account that as this new regulation will protect the data of all EU citizens, it will apply to all companies worldwide that process data of EU citizens. This may be the case, for example, when your company has a webshop that offers goods or services. P