INFORMATION SHEET No.134

Overview: How will the new EU Data Protection Law affect companies? *November 2017*

Introduction

The European Union legislated the Data Protection Directive 95/46/EC in order to provide a shield for the right to privacy and the protection of personal data. The Directive preserves two significant ambitions of the European integration process; the fundamental right to data protection and the achievement of the internal market; the free flow of personal data. The rapid technological developments however, and globalisation have profoundly changed the world around us, and brought new challenges for the protection of personal data. After years of preparation and debate, the EU General Data Protection Regulation (GDPR) was finally approved on 14 April 2016 and published in the EU Official Journal on 4 May 2016. It will apply directly in all EU Member States from 25 May 2018. It will repeal and replace Directive 95/46EC and its Member States implementing legislation. The new Regulation is an effort to modernise data protection law across the region, to provide a uniform set of rules to be applied consistently in all member states and to address privacy issues arising out of the collection, storage, processing and use of personal data.

What is personal Data?

Personal data is any information related to a natural person or "Data Subject" which can be used to directly or indirectly identify the person. Data Subject is a natural person whose personal data is processed by a controller or processor. The "Data Controller" is the entity that determines the purposes, conditions and means of the processing of personal data. "Data Processor" is the entity that processes data on behalf of the Data Controller. A simple email address, a photo, even it cannot reveal the identity of its owners, as well as the bank details, online habits of a person that can create his profile, amounts to personal data. In addition, "Sensitive Data" means data of ethnic origin or racial, political opinions, religious or philosophical beliefs, participation in a union, club or trade union organisation, health, sexual life and sexual orientation, and anything about criminal prosecution or conviction.

Main Reforms

The GDPR introduces the following major reforms to the data protection law:

Territorial scope

One of the most crucial changes of the regulatory landscape of data privacy comes with the extended jurisdiction of the GDPR. Many companies based outside the EU that are processing personal data about persons who are in the EU will need to comply and appoint a representative in the EU. Moreover, the GDPR will apply to non-EU establishments where data about Data Subjects who are in the EU is processed in connection with "offering goods or services" or "monitoring" their behaviour.

Privacy by Design

The controller shall implement appropriate technical and organisational measures in an efficient way in order to comply with the Regulation and to protect the rights of Data Subjects. According to Art. 23 controllers shall process only the necessary data for the completion of its duties (data minimisation), as well as limiting the access to personal data to those needing to act out the processing.

Data governance and accountability

The concept of accountability is at the heart of the GDPR rules. Companies will need to be able to demonstrate that they have analysed the GDPR's requirements in relation to their processing of personal data and that they have implemented a system or programme that allows them to achieve compliance. Data protection must be by design and by default. Processes must be subjected to privacy impact assessments and be well-documented.

Consent

Consent must be explicit and limited. Data Subjects have the right to request their data, rescind that request, and be forgotten. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language.

Appointment of Data Protection Officer

According to Art.37 of GDPR a Data Protection Officer must be appointed in the case of: (a) public authorities, (b) organizations that engage in large scale systematic monitoring, or (c) organizations that engage in large scale processing of sensitive personal data. The Data Protection Officer assumes the tasks of advising, monitoring internal compliance and cooperating with the supervisory authority and is bound by secrecy and confidentiality.

Penalties

Under GDPR the maximum fines for non-compliance are the higher of €20m and 4% of the organsation's worldwide turnover. This is the maximum fine that can be imposed for the most serious infringements; not having sufficient customer consent to process data or violating the core of Privacy by Design concepts. Additionally, a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and Data Subject about a breach or not conducting impact assessment.

Breach Notification

Under the GDPR, breach notification will become mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This must be done within 72 hours of first having become aware of the breach. Data Processors will also be required to notify the controllers, their customers, "without undue delay" after first becoming aware of a data breach.

Data Portability

GDPR introduces data portability; the right for a Data Subject to receive the personal data concerning them, which they have previously provided in a "commonly use and machine readable format" and have the right to transmit that date to another controller.

The Right to be forgotten

The conditions for erasure are defined in article 17. A person can simply withdraw their consent to have their data processed and the data concerning them should be deleted.

What do you need to do to comply with this Regulation?

1. Nominate a Data Protection Officer within your company.
2. Examine your organisation's data breach procedures and have a clear plan of action should a data breach occur. Ensure that those responsible for putting the plan into action know who to notify within the relevant time lines.

3. If your business is based outside of the EU, the appointment of a data protection representative who is based within the EU, should take place.
4. Review internal data protection policies. Training might be required for the staff members of the company to ensure their dealings with personal data are legally compliant.
5. In commercial agreements, examine the data protection risks and apportion risk at an early stage between the parties involved.
6. Ensure that data protection policies are easily accessible and are transparent to individual data subjects.
7. Review all consents received for direct marketing campaigns and ensure they fit within the new definition of "consent". Modify the method that consent is obtained from clients so that consent is demonstrated by an affirmative action.

Concluding Remarks

The provisions of the GDPR ensures that standards of protection of personal data have been enhanced with tools, which safeguard privacy, and indicate that will provide more control to the individuals over their personal data. The controllers and processors also must take significant efforts to comply with the provisions of the new Regulation. The impact of the Regulation however will have to be examined in the near future.

NOTES

The above is intended to provide a brief guide only. It is essential that appropriate professional advice is obtained. Totalserve Management Ltd will be glad to assist you in this respect. Please do not hesitate to contact us.