GDPR, the clock will still be ticking after 25 May 2018.

news
finance, *26 July 2018*

For many companies, GDPR is a word they don't know or prefer not to hear. However, every company will need to be GDPR compliant as of 25 May 2018. Therefore, it is important that you are aware of the obligations and the sanctions that the GDPR contains.

GDPR, what is it and why?

GDPR is the abbreviation for "*General Data Protection Regulation*". It concerns a European regulation that aims to protect the personal data of natural persons. The GDPR was established because of the digitalisation of our world. Protection of personal data is very important in this matter. Companies like Facebook and Google process a lot of personal data, but they are not alone. We can be quite sure that almost every company does this.

The second reason why the European regulation was established is for uniformity. Before the regulation there was already a European guideline. This was converted into national law in every member state, with too many differences between the member states. For this reason the European Union chose to issue a regulation. This regulation is applicable immediately in every member state.

Scope of the GDPR

The regulation is applicable as soon as the personal data of a natural person is electronically processed or is arranged in order (alphabetically, chronologically). Processing should be interpreted broadly. Examples are ordering, collecting, storing and processing.

The regulation also provides some exceptions to the scope of application. The processing of personal data in the context of activities which are outside the scope of Union Law, or activities carried out by a natural person in the course of purely personal or household activity, do not fall within the scope of application. Also, the processing by a member state in the context of the policy for border control, asylum and immigration is not targeted by the regulation.

Regarding the territorial authority, this extends beyond the EU. First of all, the controllers and

processors who are in the EU must comply with the regulation. The regulation also has an impact on the controllers and processors outside the EU. They must always comply with the regulation to the extent that they process personal data of people who are in the Union.

More rights for the data subjects

The big aim of the regulation is to provide more protection to the natural person regarding his personal data. This protection is associated with providing information, exercising control as well as granting rights.

The data subject, whose personal data is processed, must obtain transparency. This means that the data subject must be informed in good, clear and understandable language. The regulation itself provides explicitly what must be included in this information. (Art. 13 and 14 GDPR)

In addition, the regulation foresees that the data subject has more control over the processing of his personal data. This is achieved by the rights which are granted to the data subject. These rights are: transparency, rectification, inspection, deletion, limitation, objection, free transfer and automated decision-making. By means of being able to exercise these rights, the data subject has the possibility to control the processing of his personal data and possibly taking action.

If all this is not enough, the data subject can lodge a complaint with a supervisory authority or apply to the courts. For Belgium the supervisory authority is Privacy Commission.

Obligations arising from the GDPR

In addition to the protection of personal data of the data subject, there are more and more stringent obligations for the controller (and processor). First the controller must be able to show that they are GDPR compliant. This means that the burden of proof regarding the compliance of the obligations rests with the controller. In order to show this, the controller must establish an internal policy.

This internal policy ensures that the other obligations of the regulation are complied with. These other obligations are the guarantees of the rights, procedures regarding data leaks and the exercise of rights by the people concerned, establishing a register of processing activities, privacy declarations, making contracts conform (employees, customers, suppliers, ...), improving the security of the IT systems, etc.

Is this not going too far?

Despite the best intentions of the regulation, this is all very far reaching. Everybody agrees that the protection of personal data is essential in a digital world. However, the regulation has also dragged small companies into its gigantic web of obligations. Think about the baker just around the corner, who processes your personal data with the objective of preparing your

order or binging it to your home. He is also subject to the regulation.

The fact that the regulation provides for proportionality, is only a meagre consolation. The regulation certainly allows that the obligations only have to be complied with in proportion to the possibilities of the company. However, compliance remains a difficult feat for many companies.

Conclusion

The GDPR applies to almost everyone. You cannot afford to ignore the regulation as the sanctions are not small. The administrative fines can amount to EUR 20,000,000 or 4% of the global revenue of the previous fiscal period if this is higher. The Privacy Commission will perform the audits using investigation and prosecution powers. The risk of an audit increases indeed if a data subject files a complaint.

Nesrine Jelti
info@atern.io