BOYANOV & Co.
ATTORNEYS AT LAW

82, Patriarch Evtimii Blvd., 1463 Sofia, Bulgaria
T +359 2 8055055 F +359 2 8055000
E mail@boyanov.com www.boyanov.com

ALERT

On 25 May 2018 the new General Data Protection Regulation (2016/679) (the "**GDPR**") will enter into force.

How is this important to you?

While the GDPR mostly upgrades the current legal regime after 20 years of case law and practice on personal data protection, its entry into force will introduce **significant new fines** reaching **up to the higher of €20 million or 4% of the annual worldwide turnover**.

Until now many businesses have neglected the personal data protection legislation due to the relatively low sanctions (the highest fine issued to date by the Bulgarian data protection authority has been BGN 47,000). This will change after the GDPR enters into force.

What should you do? When?

The first steps to make sure you avoid the above hefty fines after 25 May 2018 are as follows:

Check whether you fall under the GDPR

If you collect and handle personal data you are likely to fall within the realm of the GDPR. For example, if you collect data about the name, age, gender, address, telephone number, etc. of your customers, employees or contractors you are collecting personal data. Compared to the previous legal regime the GDPR has broader scope and is mandatory not only to EU companies, but also to non-EU companies targeting or monitoring EU citizens.

If you fall under the GDPR check what you must do to comply with the GDPR

Do not assume that you are GDPR compliant just because you had implemented measures to comply with personal data protection legislation that existed before the GDPR.

Identify what your data processing activities and internal policies are and whether they comply with the current legal regime.

Many companies in Bulgaria are not fully compliant with the existing data privacy laws, whether due to neglecting data privacy laws or because the cost of compliance so far outweighed the potential risks. With the entry into force of the GDPR this will change due to the hefty fines for incompliance.

The broad definition of "personal data" is causing confusion. "Personal data" is any information relating to an individual that may allow their identification – not only the name, personal identification number and address, but also information related to the individual's profession, health, hobbies, image, etc.

In some cases, even data related to legal entities could be "personal data" – for example, a director of a company signing an agreement that contains his name, signature and other individual details.

Consequently, an archive containing signed agreements would be a database containing personal data and would need to adhere to the standards for protection of personal data.

One of the main principles of personal data protection is the minimisation of processed personal data – a controller is legally allowed to collect only the absolute minimum required to achieve a set purpose. For example, collecting copies of ID cards or passports, unless expressly required by law, is viewed as disproportionate as the identification could be achieved by looking at the ID document and writing down the necessary details, without making a copy.

Processing of the so-called "sensitive personal data" is strictly regulated by law. "Sensitive" are the categories of information the processing of which is considered highly invasive – data on religion, political beliefs, health, trade-union membership, etc. Collection and further processing of such data is permitted only after the personal data regulator's prior approval, even where collection of such data is required by law – e.g. an employer collecting sick leave certificates from his employees without prior approval would violate the law (even though not collecting them would be a violation of another law).

Conduct a due diligence on compliance with data protection laws well in advance of 25 May 2018

Such due diligence would assess the adequacy of data protection in your organisation, will identify any potential violations and risks associated with them and will suggest actions to bring your organisation in compliance with data protection laws. The ultimate goal is to avoid or mitigate the risks of hefty fines after 25 May 2018.

For more information please contact Damian Simeonov, partner, at email d.simeonov@boyanov.com