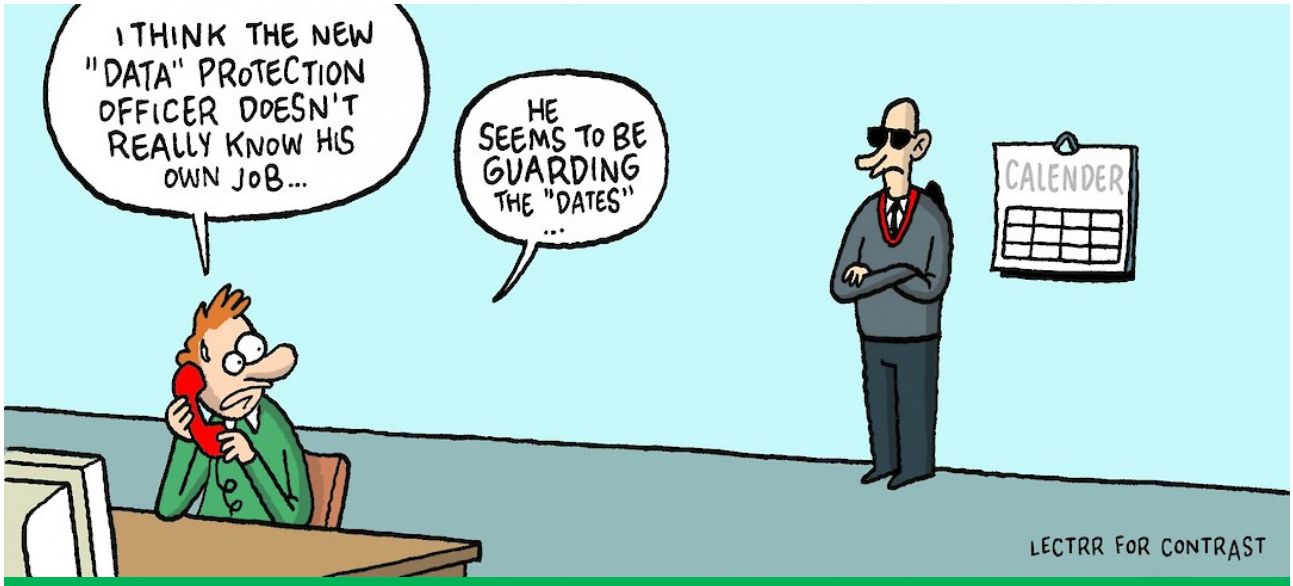
contrast



Privacy / Data Protection – Companies: 1 – 0

November 2016

Imagine...

Like every day, around 12.30 you saunter off to your company's cafeteria to eat lunch with your colleagues. Today, however, you immediately notice that their discussion is a bit more animated than usual. Jan from Human Resources is talking about an extensive exercise that will have to be held, with the possible appointment of a *DPO* and the performance of a *DPIA*. Sofie from Marketing observes that the introduction of the *GDPR* gives extensive powers to the *DPAs*, with an *EDPB* at the European level. Marc, the compliance officer, looks serious and mutters that, in light of the sanctions that are provided, he's already being pressured by the management to make sure that the company gets into compliance with the new rules pronto.

It dawns on you that you have not the foggiest idea of what they are talking about … *DPO*, *DPIA*, *GDPR*? Sanctions?

contrast

A brief clarification.

More than 4 years after the European Commission promised that it would reform the EU rules on the protection of personal data, the **new General Data Protection Regulation** ("*GDPR*") was adopted on 24 May 2016. The GDPR applies to all companies established in the European Union as well as to companies established outside the European Union that offer services within the European Union. Companies have been given until 25 May 2018 to bring themselves into line with the new personal data protection rules.

What's the GDPR all about?

The GDPR replaces the system of reporting to the national privacy authorities ("Data Protection Authorities", abbreviated "*DPAs*"), which currently exists in many Member States, with a new "**accountability**" system. Companies shall themselves have to verify whether their processing of personal data is in line with the GDPR. One aspect of this is the obligation to keep a **register with all processing activities** that occur under the company's responsibility. In addition, for certain processing activities the GDPR provides for a prior **data protection impact assessment** ("*DPIA*"). Depending on the processing activities they perform, some companies will also have to appoint a **data protection officer** ("*DPO*"). The GDPR introduces a number of **other obligations** as well: companies must provide a great deal of information to the parties involved (the "data subjects") about the processing of their personal data; strict rules apply concerning the response given to data subjects who wish to exercise their rights (to access, rectification, etc.); agreements with processors of personal data (e.g. server providers) are required to include certain clauses; data breaches must be reported to the privacy authority within a certain period, and so on.

What are the sanctions?

Several DPAs, including the Belgian Privacy Commission, do not presently have the power to impose fines. By contrast, violations of the new GDPR can be sanctioned with administrative fines up to 20 million EUR or 4% of the total worldwide annual turnover of the company in the preceding financial year, if the latter figure is higher. These fines can be imposed by the competent DPA, which is receiving investigative and prosecutorial powers that are very similar to the existing powers of competition authorities. Thus DPAs will be able to address requests for information to companies and conduct on-site inspections ("dawn raids").

How to avoid them?

The venerable adage that an ounce of prevention is worth a pound of cure applies to privacy law as well. It is important that companies take action *now* so as to ensure that the processing of personal data is in compliance with the GDPR by 25 May 2018. Moreover, a clear compliance policy can help prevent violations of the GDPR.

Concretely.

You can consult the “ABC of the GDPR” here.

What must your company do before the GDPR enters into effect on 25 May 2018?

- Firstly, you must systematically identify all processing activities that are performed within the company (both with regard to the personal data of employees and suppliers / customers and consumers).
- Then, for each processing activity, you must verify whether it is in compliance with the GDPR, by asking e.g.: is there a lawful ground for this processing? Were the data subjects properly informed? Is the data being correctly stored? As applicable, you must do whatever is necessary in order to ensure compliance with the GDPR.
- At the same time, it would be best to draw up an internal compliance policy containing procedures for e.g. initiating processing activities, maintaining a register of processing activities, following up on requests from data subjects and reporting data breaches. You must train the involved parties within the company so that they fully understand the compliance policy and are able to effectively apply it in practice.

Want to know more?

Consult the website of the Belgian Privacy Commission or the Article 29 Working Party and the “ABC of the GDPR" of **contrast.**