What employers need to know about the GDPR!

The European General Data Protection Regulation (hereinafter referred to as the GDPR) was adopted on 27 April 2016. It will enter into force on **25 May 2018**.

Harmonizing the fragmented personal data protection landscape in Europe, the GDPR is an attempt to address the digital developments that are currently unfolding, by:

- Tightening the obligations of companies regarding the processing of personal data;
- Strengthening the rights of individuals concerning their personal data and by introducing new rights;
- Strengthening the control mechanisms (and sanctions) when the protection of personal data is at stake.

GDPR: a forewarned employer…

Employers process all kinds of data belonging to their employees, starting with the creation of a file, the CV and letter of application of the future employee. Other personal data are processed daily for the administration of staff: the personal number, pay data, attendance records, etc.

Personal data are **all the data pertaining to a person who is – or may be – directly or indirectly identified.**

As soon as these data are **processed** materially or digitally, they fall under the GDPR. The term "processing" has a very broad meaning that covers in particular the collection, recording, editing, consultation, use and communication by transmission.

In its capacity of **employer,** the company is the **data controller**. It decides why and how the personal data of its employees are processed.

The company may opt to outsource the payroll management to a service provider, in which case the latter becomes a **subcontractor** acting on behalf of the controller.

Obligation of information incumbent on employers

The tightening of the GDPR regarding the obligations of employers is clearly expressed in the obligation of information and documentation incumbent on them. Employers are required to consider how they collect and protect personal data.

What type of information must the employer communicate and when?

Employers must provide specific information to employees concerning the processing of personal data.

Employees must know:

- Which personal data concerning them are processed and what the purpose of that processing is;
- Whether the data come from the employees themselves or other sources;
- Who will be authorized to consult said data;
- How long the data will be kept;
- Whether their data are sent outside the EU and if so, what their rights are;
- Whom they can contact about the processing of their data;
- What rights they have to check the processing of their data.

The latter point is one of the key issues of the new regulation. The GPPR is intended to increase transparency in personal data processing for the persons concerned. Employees must therefore be informed what happens to their personal data and to what extent they are protected. They must therefore not only be kept informed of the processing of their personal data, but must also know that they are entitled to access and, where necessary, correct, delete, and limit said data, or to lodge a complaint.

Employers must communicate such information to their employees each time they collect personal data concerning them, unless the employees already have that information.

How to proceed in concrete terms

A confidentiality policy sets out the rights of employees and informs them about the processing of personal data concerning them. Drafting such a policy, where all this information is clearly stated, will in theory enable employers to meet the obligation of information for the entire term of the contract with the employee.

Securex wants to provide a sample confidentiality policy document.

Establishment of a register of processing activities

In parallel with the aforementioned information, in certain cases the GDPR requires companies to keep a record of the processing activities they carry out.

This obligation applies in theory only to companies with at least 250 employees. As such, the GDPR aims to spare small and medium-sized companies of this red tape.

Nevertheless, the smallest companies must nonetheless keep a register as soon as the procession is no longer occasional and likely to entail a risk for the rights and freedoms of the persons concerned.

Attention! Personnel management is not “occasional processing.” Therefore, all employers, irrespective of the size of the company, must take the precaution of keeping such a register for the processing of the personal data of their employees.

This register must contain a certain number of information items, such as the:

- Purpose of the processing (for example, the payment of salaries);
- Categories of personal data processed (e.g. financial data);
- Addressees or subcontractors to whom the data were or will be transmitted (e.g. the payroll provider);
- Period during which the data will be kept;
- ….

The GDPR has not devised a predefined model for this register of activities. It is however possible to create such a register in the GDPR Compliance Support Tool developed by the Commission Nationale de Protection des Données (CNPD) [National Data Protection Commission] https://cst.cnpd.lu/portal/.

The time has come for action!

The entry into force of the GDPR will have an impact on companies and more specifically on their information processing procedures. They have a few weeks left to fall in line and adapt the internal organization of their human resources. In the event of non-compliance with the protection of data, the CNPD may impose administrative fines. Such fines may in certain cases amount to as much as €20 million or 4% of a company’s worldwide annual turnover.