Ius Laboris Belgium Global HR Lawyers
Claeys & Engels

Newsletter: **The Belgian Data Protection Act comes into force today**

September 2018

Table of contents

Dear reader,

The European General Data Protection Regulation – better known under the abbreviation “GDPR” – became applicable on 25 May 2018.

Companies should in the meantime have taken the necessary steps to align their processing activities with the GDPR and frame them in the right manner.

The main rules of the GDPR were already discussed in our Newsletter of 4 May 2016. We have also gathered a lot of information about the GDPR on our website www.gdprbelgium.be.

Although the GDPR aims at a harmonisation of the rules concerning data protection within Europe, scope is also left for Member States to determine their own priorities and to lay down specific rules in national legislation, for example in the field of employment law. Of course, this must be done within the bounds of the GDPR.

Today, the long-awaited Belgian Act on the protection of physical persons with regard to the processing of personal data (“Data Protection Act”) was published in the Belgian State Gazette. This act replaces the previous Data Protection Act of 8 December 1993 and comes into effect today.

Below, you will find a summary of the most important rules that have an effect on almost all companies.

We hope you enjoy the read!

1 Scope

The Belgian Data Protection Act is firstly applicable to processing in the framework of the activities of the Belgian establishment of a processor or controller, regardless of whether the processing takes place in Belgium or not.

An exception to this applies to a Belgian processor who acts on behalf of a controller from another EU Member State, and the processing also takes place in this other EU Member State. In this case, the law of this other EU Member State applies.

However, the Belgian Data Protection Act can also apply to non-European companies that do not have an establishment in Belgium. This is the case when a company:

- offers goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in Belgium;
- monitors the behaviour of persons in Belgium, through e.g. online profiling.

2 Sensitive personal data

According to the GDPR, a number of special categories of personal data benefit from a specific regime because of their sensitive nature: genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data revealing racial or ethnic origin, political opinions, religion or beliefs, or trade union membership, and data concerning someone's sexual behaviour or sexual orientation. Also, a specific regime applies for data concerning someone's criminal past, demonstrable in Belgium by an extract from the criminal records.

2.1 Principle of prohibition for processing

The processing of such sensitive data is prohibited, unless the company can call upon an exception for the processing.

One of the exceptions is the necessity for reasons of substantial public interest. The Belgian Data Protection Act determines that associations and foundations for which the processing of sensitive data is necessary for the purposes of achieving their statutory objectives can call upon this exception under certain circumstances.

The other exceptions of the GDPR, for example when the processing is necessary for the purposes of carrying out the obligations in the field of employment law, will of course continue to exist alongside.

2.2 Genetic data, biometric data and data concerning health

The processing of such data is prohibited, unless a company can call upon one of the exceptions. For example, the processing of such data is possible when someone has given his/her explicit consent for this. However, in the framework of an employment relationship, consent risks being invalid because its free nature can be contested.

In the field of employment law, the GDPR provides for the possibility for Member States to determine additional exceptions for the processing of such data. Some countries have taken advantage of this possibility to allow under certain conditions access control by means of e.g., a finger print or retinal scan. However, in the Belgian legislation, such an exception is not included, and the Data Protection Act does not contain this possibility either. For employers, it will therefore remain difficult to use biometric authentication systems for access controls and time registration, taking into account that the situation should be assessed on a case-by-case basis.

For the processing of genetic and biometric data and data concerning health, the new Data Protection Act confirms the additional conditions which already existed on the basis of the rescinded rules. In particular, there exists an obligation to draft a list with

categories of persons who have access to these data and a description of their role in the framework of this processing. The company must be able to present this list to the Data Protection Authority ("DPA") if it so requests. The persons who have access should further be bound by a statutory or contractual confidentiality obligation.

2.3 Criminal data

The processing of data concerning the criminal past of persons, such as an extract from the criminal records, is in principle prohibited.

The Data Protection Act currently provides some exceptions to this. For example, processing of criminal records is possible:

- when this is necessary for the management of own disputes;
- by solicitors or other legal advisers, to the extent that the defence of the interests of their clients requires this;
- for reasons of substantial public interest for the purposes of carrying out tasks of public interest which are stipulated by an act, decree, ordinance or European law;
- when the person concerned has clearly made this data public on his/her own initiative for one or more well-defined purposes;
- when the person concerned consents to this. In our view, however, this exception can not be used by employers. Because of the subordinate relationship in an employment relationship, the consent can after all be considered as being not freely given and therefore invalid. Yet, this new exception does offer opportunities in other situations than the employment relationship. You will then have to ensure that the consent meets the strict conditions of the GDPR: consent must be free, specific, informed and unambiguous and be written in clear, understandable language.

With regard to the prohibition and the strict exceptions, employers from the private sector will in principle not be able to retain an extract from the criminal records of employees or job applicants, unless one of the aforementioned exceptions applies.

We remind you that the DPA has indicated in the past that you may in the other cases ask a (candidate) employee to show an extract from the criminal records voluntarily, but you may not take a copy or take notes of it or retain it.

3 Provision of information society services to children

According to the GDPR, children below the age of 16 years must receive consent from their parents to gain access to 'information society services' such as social media, websites, apps, etc. The responsibility of verifying this lies with the providers of these services. However, Member States may provide for a lower age provided that such lower age is not below 13 years, and Belgium has made use of this possibility.

In light of the Belgian Data Protection Act, children as of the age of 13 years will therefore themselves have to give their consent for any processing of their personal data when they make use of social media, websites, apps, etc.

The DPA had given positive advice on the lowering of this age to 13 years as this age is more in line with the daily reality where many young people already go online from a young age.

4 Derogations for processing for historical, statistical or scientific purposes

To facilitate scientific and historical research and the production of statistics, Member States can provide in their national legislation derogations from the following rights: access, rectification, restriction and objection. However, the derogation regime can only be applied in so far as the above rights are likely

to render impossible or seriously impair the achievement of the specific knowledge purposes, and such derogations are necessary for the fulfilment of those purposes.

The above processing for knowledge purposes must be interpreted broadly. It concerns not only research activities in an academic framework, but also research & development activities of companies, no matter how small. An example quoted by the Data Protection Authority in its advice concerning the preliminary draft of the Data Protection Act is a company that invites a group of consumers to gauge if newly developed packaging is more user-friendly than the current packaging. According to the Data Protection Authority the impact is thus not limited to universities or specific innovation-oriented companies, but also includes small-scale research activities. However, the parliamentary preparation of the act shows that not all members of the government agree with this view and that according to them only scientific research in the strict sense would fall under the derogations. According to this view, the derogations only apply when the scientific research serves the public - and not just a private - interest .The precise scope of these derogations will therefore have to be further clarified.

In order to be able to apply the exception regime of the GDPR, the Data Protection Act determines the safeguards below, which entail additional obligations for all companies that carry out processing for knowledge purposes as explained above.

4.1 Anonymisation or encryption

According to the GDPR, encryption can be an appropriate safeguard to protect personal data, and anonymisation must be applied where possible.

In line with the former regulation, the Data Protection Act goes a step further and introduces a type of cascade system:

- data must be anonymised to ensure the persons concerned can no longer be identified;
- when this is not possible, data will have to be encrypted or encoded (so-called “pseudonymisation”). As a result, data can no longer be linked to a specific person without additional data being used. These additional data must be stored separately and be adequately secured;
- only when encryption is not possible either can unencrypted data be used. However, unencrypted data may not be distributed or communicated to third parties.

4.2 More extensive records of processing activities

Companies that process personal data for knowledge purposes have to add the following elements to the records of processing activities:

- the justification of the use of the (un)encrypted data;
- why the exercise of the right to access, rectification, restriction and/or objection by the data subject is likely to render impossible or seriously impair the achievement of the knowledge purposes;
- in case of processing of ‘sensitive data’, the data protection impact assessment (if applicable).

4.3 More extensive information obligation

In the framework of the GDPR, the controller must provide a lot of information to the persons whose data he/she processes. Companies that process data for knowledge purposes will have to provide information about two additional elements if they collect the data directly from the data subject:

- the fact that the data are anonymised or not;
- why the exercise of the right to access, rectification, restriction and/or objection by

the data subject is likely to render impossible or seriously impair the achievement of the knowledge purposes.

If the data are not collected directly from the data subject, an agreement will have to be concluded with the controller for the original processing (from whom the data are obtained) or, in case of exemption from concluding an agreement, a notification to the latter should be made. These documents must also be added to the records of processing activities.

5 Data Protection officer: additional obligations

By virtue of the GDPR, some companies, such as public authorities or companies whose main activity exists in large-scale processing of sensitive data (e.g., hospitals) or in systematic large-scale monitoring of persons (e.g., insurance companies) are obliged to appoint a 'data protection officer' (DPO).

The Data Protection Act adds two more possible cases for the compulsory appointment of a DPO:

- a company or institution that carries out processing for scientific or historical research or for statistical purposes;
- a private company that processes personal data on behalf of a federal authority or to which a federal authority transfers personal data.

In line with the risk-based approach of the GDPR, a DPO will only have to be appointed in these two cases if the processing of these data can entail a 'high risk'.

For the meaning of 'high risk', reference is made to the obligation to carry out a 'data protection impact assessment' ("DPIA") for high-risk processing activities.

The GDPR does not provide a definition of the concept of 'high risk'. The European Data Protection Board or EDPB (formerly: Article 29 Working Party), the overarching European body of supervisory authorities, and the Belgian DPA have clarified this concept in their opinions and listed a number of situations in which a DPIA is always required, such as in case of large-scale processing of biometric data, e.g., in the framework of genetic research.

For further information about this obligation to carry out a DPIA, see our Newsflash of 28 March 2018.

6 Legal remedies

6.1 Overview

Individuals who believe they are subject to an infringement of the legislation concerning data protection or feel impaired in the exercise of their rights have the following legal remedies:

- a complaint with the competent DPA (not necessarily the Belgian DPA);
- an action for injunction before the court to have the infringement stopped;
- a legal claim before the court.

The Belgian Data Protection Act provides for the possibility of being represented in this by an organisation or association active in the field of data protection. This organisation or association can then lodge a complaint or go to court on behalf of the natural person(s) concerned. However, this organisation or association must be given instruction and can not bring a case before the DPA or the court on its own initiative.

6.2 Action for an injunction

When a person or the DPA wants to stop an infringement of the legislation concerning data protection or enforce the exercise of its rights, it can file an injunction order before the president of the court of first instance, who is judging in summary proceedings. Consequently, it is a procedure with shortened deadlines to enable quick action.

The president of the court of first instance can impose the following measures in an injunction order:

- set a deadline to put an end to an infringement or grant a request for the exercise of rights;
- disclosure: posting of the judgment (or a summary thereof) within or outside the company and/or its publication in the press;
- if inaccurate, incomplete or irrelevant personal data or personal data of which storage is prohibited were communicated to third parties, the processor or controller can be obliged to notify these third parties of the restriction, rectification or deletion of these personal data.

If there are compelling reasons to fear that evidence in support of an action for injunction would disappear or be made inaccessible, the plaintiff can request through a unilateral petition the president of the court of first instance to order measures to prevent such disappearance or inaccessibility.

7 Sanctions

The GDPR requires a system of sanctions that are effective, proportionate and dissuasive.

7.1 Administrative sanctions

Companies that flout the rules can be heavily fined by the DPA with administrative fines of up to EUR 20 million or 4% of the annual worldwide turnover of the company.

The DPA can also impose corrective measures:

- warning
- reprimand
- obligation to grant requests for exercising of rights;
- obligation to bring processing in line with the provisions of the GDPR;
- obligation to communicate a data breach to the person concerned;
- temporary or permanent processing restriction, including a prohibition for processing;
- obligation to rectify or erase personal data;
- obligation to suspend data flows to a third country.

With the Data Protection Act, Belgium has made use of the possibility provided by the GDPR to exclude the government from the regime of administrative fines, with the exception of the public bodies which offer goods or services on the market.

7.2 Criminal sanctions

On the basis of the Data Protection Act, certain infringements can also be subject to criminal sanctions. Moreover, not only the controller or processor, but also their appointee or authorised representative risks a penalty; however, the controller or processor is civilly liable for the payment of fines that their appointee or authorised representative has been ordered to pay.

A penalty of EUR 2,000–120,000 can be imposed for the following infringements:

- processing without legal ground;
- violation of the basic principles with regard to processing of personal data, with severe negligence or malevolence;
- continuation of a processing to which objection has been made without compelling legitimate reasons;
- transfer of personal data outside the European Economic Area without adequacy decision or appropriate safeguards, with severe negligence or malevolence;
- violation of a temporary or permanent processing restriction imposed by the DPA;
- disobeying a corrective measure imposed by the DPA;
- impairment of the supervision of or resistance to the DPA;

- use of false certification or certification of which the period of validity has expired.

A company that forces a person to consent to a processing of his/her personal data by using violent acts, violence, threats, gifts or promises can be fined between EUR 800 and EUR 160,000.

Furthermore, the correctional court can also order that a judgment be published in one or more newspapers.

The rescinded rules already provided for criminal fines, but in practice these were rarely applied. The degree of these fines and the risk that they are imposed is now higher.

Nevertheless, it is noteworthy that the maximum amount of the criminal fines is significantly lower than that of the administrative fines. In other fields, such as social criminal law, it is customary that the degree of administrative fines is lower than the criminal fines, which counts as the last resort. In its opinion on the preliminary draft of the Data Protection Act, the DPA had recalled that the level of sanctioning laid down should allow reacting in an effective, proportionate and dissuasive manner. Time will tell if these levels of sanctioning effectively will have the desired effect. In any event, we believe that it will also have an impact on the interaction between, on the one hand, the DPA, who can impose the administrative fines, and on the other hand, the public prosecutor, who can decide to summon before the correctional court.

7.3 Concurrence of administrative and criminal proceedings

For infringements for which both an administrative and a criminal sanction are possible, the Data Protection Act has determined some procedural rules to avoid a situation in which a company receives both sanctions for the same infringement.

The public prosecutor can take action first and start a preliminary investigation, order a judicial inquiry and/or institute criminal prosecution before the criminal courts. The public prosecutor has a period of two months as of the day of receipt of the official report to communicate the starting of criminal proceedings to the DPA. During this period of two months and when the public prosecutor effectively takes on the file, the DPA no longer has the authority to exercise its corrective powers and consequently a (high) administrative fine can not be imposed. However, when the public prosecutor lets this period of two months pass, only an administrative sanction will still be possible.
The above rules will only apply to the extent that no other working arrangements are laid down in a protocol agreement between the public prosecutor and the DPA.

Brussels
boulevard du Souverain 280
1160 Brussels
Tel.: 02 761 46 00
Fax: 02 761 47 00

Liège
boulevard Frère Orban 25
4000 Liège
Tel.: 04 229 80 11
Fax: 04 229 80 22

Antwerp
City Link
Posthofbrug 12
2600 Antwerp
Tel.: 03 285 97 80
Fax: 03 285 97 90

Ghent
Ferdinand Lousbergkaai 103
box 4-5
9000 Ghent
Tel.: 09 261 50 00
Fax: 09 261 55 00

Kortrijk
Ring Bedrijvenpark
Brugsesteenweg 255
8500 Kortrijk
Tel.: 056 26 08 60
Fax: 056 26 08 70

Hasselt
Kuringersteenweg 172
3500 Hasselt
Tel.: 011 24 79 10
Fax: 011 24 79 11

Partners with you.