SIMONT
BRAUN

GDPR – ARE YOU READY?

MARCH 2018

On 10 January 2018, the law of 3 December 2017 concerning the establishment of the **Data Protection Authority** was published in the Belgian's official Gazette. This law, reforming the current Commission for the protection of privacy, is one of the necessary legislative efforts to anticipate the entry into force of the European Union's General Regulation on the protection of natural persons with regard to the processing of personal data and of the free movement of such data (GDPR). As of **25 May 2018** all natural or legal persons, public authorities, agencies or other bodies which process personal data or organise such processing will have to comply with these new rules. What does this mean in practice?

This news aims at providing the reader with an overview of the changes brought by the GDPR and to give some insight on the necessary measures to be taken to comply with the new legislation.

Will I be affected by the GDPR?

The GDPR applies to the processing of personal data by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. Certain exceptions and limited alterations set aside, the GDPR's material scope of application is identical to the scope of the act of 8 December 1992 on the protection of privacy in relation to the processing of personal data. The latter is currently the must-go-to legislative act in Belgium. In practice, this legislation is important for nearly all undertakings, if only for the management of personnel, clients and suppliers.

The territorial scope of the GDPR includes all undertakings established within the EU, as well as, in specific circumstances, all foreign undertakings that process personal data of individuals located in the EU. The fact that your business is established outside the EU does not necessarily entail that the GDPR does not apply to it.

The major changes brought by the GDPR do not relate to the scope of application of the rules, but to the obligations imposed on data controllers and their processors, as well as to the sanctions for non-compliance with this regulation.

Key changes and what to do in practice?

1) Currently, processing personal data is frequently based on the **consent of the individual concerned** (hereinafter: the data subject). However, this consent is not always obtained under conditions that guarantee a consent of acceptable quality. Therefore, the GDPR provides for more stringent requirements to obtain an individual's consent. In the future, any company that bases processing of personal

data on the individual's consent will have to check whether:

- the consent is obtained by a statement or a clear affirmative action (which precludes, for example, the use of pre-ticked boxes);
- the consent is freely given, specific, clear and unambiguous (meaning that the data subject was duly informed of the scope of his/her consent before giving it);
- the consent refers to a processing for one or several specific lawful purposes (general and broad phrasing is not allowed);
- where consent is given in a written statement which relates to multiple subject-matters (such as the acceptation of general terms and conditions or terms of use), the request for consent should be presented in an intelligible and accessible form, in a clear and plain language, and in a way that is clearly distinguishable from the other matters;
- it can easily demonstrate that it obtained the data subject's consent (the data processor should, therefore, keep records of the consents).

The GDPR will also apply to personal data collected before its entry into force. Hence, all processing of personal data that was consented in a way that is not satisfactory to the new GDPR requirements should be regularised – meaning that the consent should be renewed in a way that meets the GDPR requirements.

2) The GDPR also provides for **enhanced obligations of information** for data controllers. In practice, it is necessary to verify whether the documents currently used by your company (e.g. charter for the protection of privacy or privacy policy) comply with the GDPR, and ensure that they include, amongst others, the following information:

- the lawful purposes and legal basis for the processing of personal data;
- the legitimate interests pursued by the data controller or by a third party when processing is based on such legitimate interests;
- as the case may be, the fact that the data controller intends to transfer the personal data to a country that is not an EU Member State, and the existence or absence of an adequacy decision from the Commission or, where applicable, a reference to the appropriate safeguards that are put into place to protect the data subjects;
- where processing is based on a data subject's consent, the right to withdraw their consent at any time;
- the data subject's right to lodge a complaint with the national supervisory authority;
- the period during which the personal data will be stored or, if not possible, the criteria used to determine the period of conservation;
- whether the provision of personal data is a statutory or contractual requirement, or necessary to enter into a contract, as well as whether the data subject is obliged to provide his/her personal data and the possible consequences of failure to provide it;
- the existence of automated decision-making, including profiling, and useful information about the underlying logic, as well as the importance and the foreseen consequences of such processing for the data subject.

3) The GDPR explicitly mentions the "**right to be forgotten**" from which all data subjects will benefit. This right will empower the data subject to ask for a complete erasure of his/her personal data under certain conditions. Although this right of erasure inchoately existed under directive 95/46/CE and was confirmed by the ECJ's ruling in the Google Spain-case, this right is given prominent placing in the GDPR. All data controllers will have to implement a

procedure to be able to respond in practice to a request of erasure "without undue delay".

4) Every data controller shall set up a procedure to **notify every recipient** of personal data of all requests of rectification or erasure of such data, as well as of every limitation of processing, unless the provision of such information is impossible or gives rise to disproportionate efforts.

5) Regarding the data subjects' rights, the creation of a **right of data portability** – which aims at the independence of customers in the online environment – is the GDPR's most innovative addition. It gives a data subject, under certain conditions, the right to receive the personal data that he or she has provided to a controller in a structured, commonly used and machine-readable format, to transmit these data to another controller. Data controllers will have to take all appropriate technical measures to be able to act upon such requests.

6) The GDPR also establishes the foundations of data protection **"by design"** and **"by default"**. To respect these principles, the data controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation. These technical and organisational measures should also ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed. These principles will not only affect the content of products, websites or mobile applications that collect personal data, but also undertakings' general business strategy. Therefore, this requires in-depth thinking by all data controllers.

7) Data controllers and processors established **outside the EU** which must comply with the GDPR requirements (because they offer products and services to data subjects within the EU or monitor individuals that reside within the EU) should **designate a representative in the EU** as a point of contact for national supervisory authorities and data subjects.

8) Another element of attention is the relationship between the data controller and the data processor. The GDPR defines the data processor as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. It provides for specific requirements that both future and existing **outsourcing agreements for the processing of personal data** will have to satisfy. These agreements should notably:

- define the subject-matter, duration, nature and purpose of the processing;
- define the type of personal data and categories of data subjects;
- mention that the processor ensures that the persons authorised to process the personal data have committed to respect the confidentiality of such data;
- include the appropriate technical and organisational measures that the processor shall take to ensure a proper level of security in light of the risk at hand;
- compel the processor to make sure that any subsequent processor implements the same technical and organisational measures;
- compel the processor that he/she deletes or returns the personal data to the controller at the end of the provision of services relating to the processing;
- make available to the controller all information necessary to demonstrate its compliance with the obligations laid down in the GDPR.

9) Every data controller should also **keep track of the processing activities** in a record containing the following information: the name and contact details of the controller; the

purposes of the processing; a description of the categories of data subjects and of personal data; the categories of recipients to whom the personal data have been or will be disclosed, including transfers to third countries; the envisaged time limits for erasure of the different categories of data; a general description of the technical and organisational security measures.

10) In case of personal data breach, the data controller must, on some occasions, **notify the breach** to the national supervisory authority. When the breach is likely to result in a high risk for the rights and freedoms of natural persons, the data controller must also notify the data subject. Therefore, the data controller has to set up procedures ensuring that such notification is made within the mandatory terms of the GDPR (in principle, notification to the supervisory authority should be done within 72 hours of the personal data breach).

11) Where a type of processing is likely to result in a high risk for the rights and freedoms of natural persons, the controller shall, prior to the processing, **assess the impact** of the envisaged processing operations on the protection of personal data. When the assessment identifies a high risk for a certain type of processing, the data controller shall, prior to the processing, ask the national supervisory authority for advice.

12) Last but not least, under specific circumstances, undertakings will have to designate a **data protection officer**. This obligations applies when processing is carried out by a public authority or body, but also when the core activities of the controller or the processor consist of (i) processing which, by nature or because of its scope and/or purposes, requires regular and systematic monitoring of data subjects on a large scale or (ii) processing sensitive data on a large scale (sensitive data are, for example, data related to health, sexual orientation, political opinions, ethnic origin or data related to criminal convictions or offences).

Sanctions?

The GDPR substantially changes the powers granted to the national supervisory authorities and the sanctions applicable. **Administrative fines** can be inflicted upon infringers of data protection regulations by the Data Protection Authority. Their amount varies depending on the gravity of the infringement. For the most severe infringements, the administrative fines can reach up to EUR 20,000,000 or, in the case of an undertaking, 4% of the total worldwide total annual turnover of the preceding financial year, whichever is higher. Moreover, the Data Protection Authority is mandated to propose settlement agreements, give warnings and reprimands, command to act upon a data subject's request to exercise his/her rights, incur changes to the processing of data or temporarily or permanently prohibit the processing of personal data.

* * *

For further contact or specific assistance, do not hesitate to contact our **Data Protection Team**: **Philippe Campolini**, **Pierre Van Achter** and **Gaëtan Goossens**.