Ius Laboris Belgium Global HR Lawyers
Claeys & Engels

Newsletter: **A couple of points of interest for employers, sectoral organisers and pension funds concerning the application of the GDPR**

September 2017

Table of contents

Dear reader,

On 25 May 2016, the General Data Protection Regulation ("GDPR") entered into force. After a transitional period of two years, these new European rules will also apply in Belgium. In our 4 May 2016 newsletter, we covered the ten things you need to know as an employer about the GDPR, followed by several newsflashes, among others about some important positions of the Privacy Commission and the Article 29 Working Party concerning the practical implementation of the GDPR. With regard to the general framework of the GDPR, we refer you to our website (www.gdprbelgium.be).

In this newsletter, we focus on some specific points of interest for employers and sectoral organisers (both referred to here as "organisers") and also for pension funds (IORPs) in the context of data processing while implementing pension plans.

After all, a pension plan cannot be managed and executed without the processing of the personal data of the plan members and their beneficiaries. Just think for instance of the calculation of the vested pension rights, the preparation of the annual benefit statements, the payment of the retirement or death benefits.

The GDPR is applicable in all European companies, institutions and organisations and has been drafted in general terms, which sometimes makes it difficult to apply these new rules to this specific context of pension plans and pension funds. Indeed, there is no one-to-one relationship. Instead, we start from a three-party relationship between the organiser, the pension institution (pension fund or insurer) and the plan members. In addition, not only the plan members that enjoy the pension promise but also their beneficiaries are to be considered as "data subjects" within the meaning of the GDPR. Even though the latter are in fact third parties with regard to the pension promise, their personal data will also be processed, which makes them data subjects in the sense of the GDPR.

Furthermore, we do not need to start from scratch. Over the past few years, organisers and pension funds have taken numerous measures in the context of the secure processing of personal data. It is important to take this into account as much as possible, and by doing so avoid additional administrative burden for the pension funds, as well as over-engineering.

In this newsletter, we focus on a couple of the specific themes that have a particular relevance for the application of the GDPR in the context of occupational pensions. In this respect, some questions will remain unanswered as a common position of the pensions sector is still to be reached. We also briefly explain which documents should be reviewed in order to be *GDPR-proof* in time.

We hope you enjoy the read.

1 Introduction - Basic principles

The GDPR mainly confirms the existing principles, but reinforces them in several aspects. The general principles will indeed remain the same. Organisers and pension funds must ensure a lawful, fair and transparent data processing that is limited to the purposes for which the data has been collected.

It is particularly important that only the data that are necessary for the management and the execution of the pension plans are processed. The pension administration should best be screened on this point, in order to erase all additional data from the databases whose processing is not necessary.

Additionally, organisers and pension funds cannot process the personal data of the plan members and the beneficiaries any longer than is necessary in the framework of the execution of the pension plan. When deciding on the conservation period, one may however also take into account possible (legal) claims that can be filed by plan members or beneficiaries after the payment of the pension, death and/or disability benefits and the applicable statutes of limitations. In practice, this might imply a (very) long conservation period running until 5 years after the payment at the time of retirement or death of the plan member concerned. On this point, it is also important to screen the pension administration and implement these changes if necessary.

Finally, the organisers and pension funds must also take the appropriate technical or organisational measures in order to guarantee that the data will be processed in a secure manner. An unauthorised or unlawful processing (e.g., by unauthorised people) or an accidental loss of data must be avoided. In this respect, one should above all take a careful look at the internal rules in order to verify whether they are still sufficiently appropriate.

2 Are organisers and pension funds joint controllers?

The qualification of the organisers and the pension fund as “controller” or “processor” is an important starting point for the implementation of the GDPR. Their obligations and responsibilities depend on the answer to this question. The controller determines the purposes and means of the processing of personal data, while the processor ‘only’ processes the personal data on behalf of the controller.

Under the current legislation, there could already be “joint controllers” when the purposes and the means of the processing were jointly determined by several (legal) persons. The GDPR now lays down specific rules for joint controllers, among others with regard to the division of their obligations or responsibilities, and also their liability towards the data subjects.

In the past, the Privacy Commission – soon to be renamed as the Authority for the Protection of Personal Data – confirmed us that in the context of occupational pensions the distinction between controller and processor is not completely clear and that there is a joint liability. Both the organiser and the pension fund have their own specific role and obligations that require them to process personal data for which they determine the purposes and the means. Consequently, under the current legislation we already assumed that the organiser(s) and the pension fund acted as joint controllers.

In our view, this qualification will be maintained under the GDPR. In this context, the GDPR states that the joint controllers must in a transparent manner determine their respective responsibilities for compliance with the obligations of the GDPR by means of an arrangement between themselves.

This division does in principle already exist today by means of the management

agreement that is concluded between the organiser(s) and the pension fund. This clause should best be re-examined in order to make sure that it is completely in accordance with the GDPR. It should among others be agreed on who will take care of the GDPR information obligations vis-à-vis the plan members and the beneficiaries, to whom the content of this arrangement should also be made available. We believe that this can be done by means of the pension plan rules, or can be included in the additional information that is made available to them (see below - paragraph 4).

Not withstanding the arrangement that is concluded between the organiser(s) and the pension fund, the plan members and beneficiaries will be able to turn to both of them in order to exercise the rights that they possess on the grounds of the GDPR (e.g., their right of access, rectification, erasure, objection and limitation). Consequently, the manner in which this will be organised should also be made a part of the arrangement.

Being joint controllers, the organiser(s) and the pension fund are jointly and severally liable towards the plan members and the beneficiaries for damage that they might suffer as a result of an infringement of the GDPR (e.g., damage as a result of a data breach).

Admittedly, they mutually have a right to redress for damages that they compensated for but for which they are not responsible, taking into account their arrangement regarding the obligations and responsibilities. In that case, the pension fund can bring recourse claims against the organiser(s) or *vice versa*. This should also be governed by the management agreement. Especially for multi-employer pension funds that are open to companies without an economic link, this will be a particular concern.

The question arises whether this will also have an impact on the administrative fines that can be imposed in case of non-compliance with the GDPR, which can amount to EUR 20,000,000 or, for companies, up to 4% of total worldwide annual turnover (in case this amount is higher than EUR 20,000,000).

In our opinion, this is not the case. Joint and several liability only applies with regard to the plan members and the beneficiaries for the damage they suffer in the context of the processing of their personal data and not with regard to administrative fines. The latter can, in our view, only be imposed by the supervisory authority (the Privacy Commission and in the future the Authority for the Protection of Personal Data) to the person that committed the infringement and not to the joint controller that is in no way responsible for the event giving rise to the damage.

3 Legal grounds with regard to the processing

Personal data can only be processed on the basis of one of the legal grounds provided for in the GDPR. It concerns the same legal grounds that already exist under the current legislation, but a number of stricter conditions will be imposed with regard to some of them.

3.1 Consent as a legal ground

This is for instance the case for the consent as a legal basis for the processing, and this with regard to both the content and the way in which permission must be given. From now on, it must be an explicit and active action. A consent that is silent or implicit will not suffice.

Furthermore, consent must be given freely if it is to serve as a legitimate legal ground. Under the current legislation, there is already a discussion on whether an employee can freely give their consent, taking into account their subordinate position vis-à-vis the employer. In this respect, the Article 29 Working Party (WP29)[1] recently confirmed in its advice

[1] The WP29 is an independent European working party that addresses issues relating to the protection of personal data and privacy. Founded in 1996, the WP29 was created by Article 29 of the Data Protection Directive (Directive

2/2017 on the data processing in the workplace that workers can only freely give their consent in exceptional circumstances, having regard to the inherently unequal balance of power. The Privacy Commission expressed a similar view on its website.

We conclude that consent should not be the (only) legal basis for the processing of employees' personal data. Furthermore, this consent can be withdrawn at any moment, which can lead to a great deal of practical problems in the pension's administration.

3.2 Execution of the individual employment contract or the collective bargaining agreement

In order to have a legal basis for the processing of the personal data, one could also refer to the execution of the individual employment contract or the applicable collective bargaining agreement.

After all, in the case of a company plan, the pension plan rules form an integral part of the individual employment contract. In the case of a sectoral pension regime, these rules are part of a CBA (collective bargaining agreement), of which the individually normative provisions are automatically incorporated in the individual employment agreement. In order to execute this individual employment agreement (including the pension promise or the pension plan rules), the processing of personal data of the plan members is necessary.

However, this legal basis cannot be used for the processing of the personal data of the beneficiaries.

3.3 Compliance with the legal obligations as a legal ground

With regard to the beneficiaries, as well as the plan members, one could refer to the legal obligations of the organiser(s) and the pension fund on the basis of the Act of 28 April 2003 governing occupational pensions (Occupational Pensions Act) and/or the Act of 27 October 2006 concerning the supervision of institutions for occupational retirement provision(IORP Act), as well as the royal decrees implementing these acts.

Even if there is no obligation to introduce an occupational pension, once the employer or the sectoral organiser decide to introduce one, the (mandatory) provisions of the Occupational Pensions Act and the IORP Act apply. In that case, the organiser(s) and the pension fund will be obliged to process the personal data of the plan members and beneficiaries in order to execute the pension promise in accordance with the Occupational Pensions Act and the IORP Act, namely the calculation of vested reserves and benefits, drawing up and distributing the annual benefit statements, payment of the pension, death and disability benefits, communication concerning the exit from the plan, the execution of individual or collective transfers.

In 2011, the Privacy Commission confirmed that compliance with the legal obligations in the context of the management of the pension obligations in accordance with the Occupational Pensions Act and the IORP Act as well as (for the plan members) compliance with the employment contract constitute legal grounds with regard to the processing of personal data. Since the GDPR made no changes to these legal grounds, we assume that this position will be maintained.

95/46/EC). It is made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission. The WP29 only has an advisory status, but its advices carry great weight because of its composition.

4 Extension of the information requirement

4.1 Additional information to be provided

According to the current rules, the organiser(s) or the pension fund need to deliver specific information about the data processing. This information concerns, among others, the purposes for which this data will be processed, the description of the data that will be processed and to whom these data will be communicated (e.g., external providers involved in the pension administration), the right of access, the right to rectification, etc.

At present, this information is usually communicated to the plan members and beneficiaries through the employment contract or an annex to this contract, the applicable sectoral CBA, the pension plan rules, the annual benefit statement or the communication concerning the payments.

Under the GDPR, this information requirement will be extended. Additional information that needs to be provided includes among others: the legal basis for the data processing, how long the data will be stored, the option to withdraw consent at any moment (if consent is (one of) the legal base(s)), the right to file a complaint with the Privacy Commission, whether the data will be transferred outside of Europe (e.g., if a part of the pension administration is handled by a non-European external provider) and the specific guarantees in that context.

As joint controllers, the organiser(s) and the pension fund should determine in their arrangement who will deliver this information.

4.2 Also to the beneficiaries?

As regards the information requirement, the GDPR makes a distinction between whether or not the data is being collected from the data subject itself. If this is not the case, one could possibly refer to an exception. In case the provision of information seems impossible or would involve a disproportional effort, it is not required. The question arises whether the organiser(s) and/or the pension fund can invoke this exception.

In this context, we believe that a distinction needs to be made between the potential beneficiaries, whose data the organiser(s) and the pension fund are already processing, and the effective beneficiaries. Think for instance of the partner and the children of the plan member, whose names and birth dates are held in the pension administration. As long as the plan member remains alive, they remain potential beneficiaries on the basis of the default beneficiary order as set out in the pension plan rules or the beneficiary form, but they cannot claim any death benefits yet and, therefore, they are not effective beneficiaries.

In an advice of 2011, the Privacy Commission ruled that the data of the potential beneficiaries are merely registered in the framework of the plan member and that these data actually ‘belong’ to the plan member. According to the Privacy Commission, the plan member can be mandated to inform their family members (potential beneficiaries) concerning the data processing in case of such an indirect registration.

Taking into account the above-mentioned exception and the view of the Privacy Commission, the position could be defended that the beneficiaries must only be informed about the data processing by the pension fund, once they are actually entitled to benefits from the pension fund (i.e. become effective beneficiaries) and directly transfer personal data to the pension fund.

5 Obligatory declaration replaced by the documentation requirement

5.1 Record of the processing activities

Under the current rules, there is an obligation to report (partial) automated data processes to the Privacy Commission.

Under to the GDPR, this obligatory declaration is replaced by a documentation duty. This means that the controller and the processor are obliged to maintain a record of the processing activities.

5.2 Not occasional processing

There is an exception to this rule. Companies or organisations employing fewer than 250 persons are not obliged to hold a record, except when the processing poses a risk to the rights and freedoms of the data subjects, involves the processing of sensitive data or when the data processing is not occasional.

Although the GDPR does not completely clarify what is meant by “not occasional processing”, it seems very difficult to argue that the data processing resulting from the management and execution of occupational pension regimes is only occasional. Furthermore, this often involves the (limited) processing of sensitive data, such as, among others, data concerning sickness and disability in the context of disability coverage.

In this respect, it should also be noted that the Privacy Commission has mentioned in its 06/2017 recommendation of 14 June 2017 concerning the record of processing activities, that personnel management cannot be considered to be an occasional form of processing.
Moreover, in our opinion, the record will prove to be a useful and even necessary instrument in the context of the implementation of the GDPR.

6 Data Protection Officer (DPO)

In the private sector, there is no obligation to designate a *Data Protection Officer* (DPO) if the personal data is only processed as an ancillary activity.

The question arises whether data processing by a pension fund could be considered to be an ancillary activity.

In the event that the organiser(s) has (have) already appointed a DPO, there will probably be no problem. The same DPO can also assume this role for the pension fund.

In case the organiser(s) has (have) not appointed a DPO, the role of information security officer (who should already have been appointed by every pension fund in the context of the minimal safety regulations concerning the information security imposed by the Crossroads Bank for Social Security) can possibly be combined with the role of DPO.

In this regard, we refer to the 04/2017 recommendation of 24 May 2017 from the Privacy Commission. In this recommendation, the Privacy Commission does not exclude the combination of the role of information security officer and DPO. It is up to the controller or the processor to determine whether this combination is admissible. The Privacy Commission does however mention that there is neither an automatic nor a systematic transition from the role of information security officer to the role of DPO and that this combination must always to be examined in each particular case. And of course, the DPO must possess the necessary expertise regarding the legislation and the practice concerning data protection.

7 Documents to be screened

Finally, we briefly go through the documents that should be re-examined by the organiser(s) and the pension funds in light of the implementation of the GDPR:

- the (possible) clause concerning data processing in the framework of the occupational pension plan in the employment contract or in the annex thereto;
- the clause in the management agreement concerning the division of the obligations and the responsibilities between the organiser(s) and the pension fund;
- the (possible) clause concerning data processing on the annual benefit statement and the other communications that are provided to the plan members and/or the beneficiaries;
- the (possible) clause concerning data processing in the beneficiary form;
- the agreements with external service providers who receive data and/or process these for the organiser(s) and/or the pension fund; on the basis of the GDPR certain additional provisions will have to be added to these agreements.

Claeys & Engels informs

At the end of this year, we will be running a workshop or a client seminar, during which we will address the implementation of the GDPR in the context of the management of your occupational pension plans even further. For this, you will receive an invitation in the next few weeks.

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.