

 **Newsletter : Quelques points d'attention pour les employeurs, les organisateurs sectoriels et les fonds de pension pour l'application du RGPD**

Septembre 2017

 **Contenu**

<b>1</b>	<b>Introduction - Principes de base .....</b>	<b>3</b>
<b>2</b>	<b>Les organisateurs et les fonds de pension sont-ils des responsables conjoints du traitement ? .....</b>	<b>3</b>
<b>3</b>	<b>Fondements juridiques pour le traitement.....</b>	<b>5</b>
3.1	Le consentement comme fondement juridique .....	5
3.2	Exécution du contrat de travail individuel ou d'une convention collective de travail comme fondement juridique .....	5
3.3	Respect d'une obligation légale comme fondement juridique .....	5
<b>4</b>	<b>Elargissement du devoir d'information .....</b>	<b>6</b>
4.1	Informations complémentaires à fournir	6
4.2	Egalement aux bénéficiaires?.....	6
<b>5</b>	<b>Obligation de déclaration remplacée par une obligation de documentation</b>	<b>7</b>
5.1	Registre des activités de traitement.....	7
5.2	Traitement des données non occasionnel .....	7
<b>6</b>	<b>Délégué à la protection des données (DPD) .....</b>	<b>8</b>
<b>7</b>	<b>Documents à vérifier .....</b>	<b>8</b>

Cher lecteur,

Le 25 mai 2016, le Règlement Général sur la Protection des Données (en abrégé: RGPD - ou, selon l'abréviation anglaise communément utilisée, « GDPR ») entrainé en vigueur.

Après une période transitoire de deux ans, cette nouvelle réglementation européenne sera également applicable en Belgique. Dans notre [newsletter du 4 mai 2016](#), nous mettions en lumière les dix choses que vous deviez connaître, en tant qu'employeur, sur le RGPD. Cette newsletter fut suivie par plusieurs newflashes portant notamment sur un certain nombre de positions importantes prises par la Commission de la protection de la vie privée et le Groupe de travail « Article 29 » concernant la mise en œuvre concrète du règlement. Pour le cadre général du RGPD, nous renvoyons également à notre site web ([www.gdprbelgium.be](http://www.gdprbelgium.be)).

Dans la présente newsletter, nous nous focalisons sur certains points spécifiques aux employeurs et aux organisateurs sectoriels (ci-après conjointement dénommés « organisateurs ») ainsi qu'aux fonds de pension (IRP's) pour ce qui concerne le traitement de données dans le cadre de l'exécution des plans de pension complémentaire.

Un plan de pension complémentaire ne peut en effet être géré et exécuté sans que des données à caractère personnel des (ex-)travailleurs affiliés et leurs bénéficiaires ne soient traitées. Nous pensons ici notamment au calcul des droits de pension constitués, à l'élaboration des fiches de pension annuelles, au paiement des capitaux de pension et de décès ou encore des rentes...

Le RGPD est applicable à tous les établissements, entreprises et organisations européens et est donc rédigé en des termes généraux, ce qui ne facilite pas toujours l'application de ces nouvelles règles au contexte spécifique des plans de pension complémentaire et des fonds de pension. En effet, nous ne pouvons pas parler, dans ce contexte spécifique, d'une relation de personne à personne. En matière de pensions complémentaires, le point de départ est une

relation tripartite entre l'organisateur, l'organisme de pension (fonds de pension ou assureur) et les affiliés. En outre, les personnes concernées au sens du RGPD ne sont pas uniquement les (ex-)travailleurs affiliés qui bénéficient d'un engagement de pension, mais aussi leurs bénéficiaires. Même si ces derniers sont des tiers à l'engagement de pension, leurs données sont tout de même traitées et ils sont donc en ce sens également des personnes concernées au sens du RGPD.

De plus, la matière ne part pas de rien. Au cours des dernières années, les organisateurs et les fonds de pension ont en effet déjà mis en place de nombreuses mesures pour un traitement sûr des données à caractère personnel. Il est important d'en tenir compte autant que possible et, de cette manière, éviter une surcharge administrative et un *over-engineering* pour les fonds de pension.

Dans la présente newsletter, nous abordons un certain nombre de thèmes spécifiques qui présentent un intérêt particulier pour l'application du RGPD dans le contexte des pensions complémentaires. Une position commune du secteur des pensions serait la bienvenue sur certaines questions qui demeurent ouvertes. Nous indiquons également brièvement les documents qui doivent être vérifiés afin d'être *GDPR-proof* dans les temps.

Nous vous souhaitons une agréable lecture!

## 1 Introduction - Principes de base

Le RGPD confirme dans une large mesure les principes existants, mais les renforce également sur un certain nombre de points. Ainsi, les principes généraux restent les mêmes. Les organisateurs et les fonds de pension doivent assurer un traitement de données licite, loyal et transparent qui se limite aux finalités pour lesquelles les données ont été collectées.

Sur ce dernier point, il est important de noter que seules peuvent être traitées les données qui sont nécessaires pour la gestion et l'exécution des plans de pension. L'administration des pensions devrait ici être passée en revue afin d'effacer de la base de données les données additionnelles pour lesquelles un traitement n'est pas nécessaire.

Par ailleurs, le (les) organisateur(s) et les plans de pensions ne peuvent pas traiter les données à caractère personnel des affiliés et des bénéficiaires plus longtemps que ce qui est nécessaire à l'exécution du plan de pension complémentaire. A cet égard - pour le délai de stockage ou de conservation - il peut être tenu compte des éventuelles actions pouvant encore être introduites par les affiliés ou les bénéficiaires après le paiement de la prestation de pension, de décès et/ou d'invalidité, et donc du délai de prescription applicable. En pratique, il peut dès lors s'agir d'un (très) long délai de conservation, qui court jusqu'à 5 ans après le paiement qui a lieu au moment de la mise à la retraite ou du décès du (de l'ex-)travailleur affilié. Sur ce point également, il est important de vérifier l'administration des pensions et, si nécessaire, de l'adapter.

Enfin, les organisateurs et les fonds de pension doivent s'assurer qu'ils prennent les mesures techniques et organisationnelles adéquates afin de garantir que les données soient traitées de manière sécurisée. Un traitement illicite ou irrégulier (par exemple, par des personnes non-autorisées) ou une perte

des données par inadvertance doivent être évités. Il s'agira surtout ici d'examiner les procédures et règles internes actuelles afin de déterminer si celles-ci sont (encore) suffisamment adéquates.

## 2 Les organisateurs et les fonds de pension sont-ils des responsables conjoints du traitement ?

La qualification de l'(des) organisateur(s) et du fonds de pension comme « responsable du traitement » ou « sous-traitant » est un point de départ important dans la mise en œuvre du RGPD. Leurs obligations et responsabilités en application du RGPD dépendront de cette question. En effet, le responsable du traitement détermine la finalité et les moyens du traitement, tandis que le sous-traitant réalise « uniquement » le traitement des données au nom du responsable du traitement.

Sur la base de la réglementation actuelle, il pouvait déjà être question de « responsables conjoints du traitement » lorsque la finalité et les moyens du traitement étaient déterminés par plusieurs personnes (morales). Désormais, dans le RGPD, des règles spécifiques ont été adoptées en cas de responsables conjoints du traitement, entre autres en ce qui concerne la répartition des tâches ou des responsabilités, ainsi qu'en ce qui concerne leur responsabilité vis-à-vis des personnes dont les données sont traitées.

Par le passé, la Commission de la protection de la vie privée - qui sera bientôt renommée Autorité de protection des données - nous avait déjà confirmé que, dans le contexte des pensions complémentaires, la dichotomie entre responsable du traitement et sous-traitant n'était pas évidente, et qu'il fallait considérer qu'il y avait une responsabilité partagée. En effet, tant l'organisateur que le fonds de pension ont un rôle et des obligations spécifiques qui les contraignent à procéder à un traitement de données pour lequel ils doivent chacun déterminer la finalité et les

moyens. Sur la base de la réglementation actuelle, nous partions par conséquent déjà du principe que le(les) organisateur(s) et le fonds de pension agissaient comme responsables conjoints du traitement.

Selon nous, cette position peut être maintenue sous le RGPD. Sur ce point, le RGPD dispose que les responsables conjoints du traitement doivent, de commun accord, préciser de manière transparente leurs responsabilités respectives aux fins d'assurer le respect des obligations issues du RGPD.

Cette répartition est en principe déjà prévue aujourd'hui dans la convention de gestion qui est conclue entre le(les) organisateur(s) et le fonds de pension. Idéalement, l'article concerné de la convention de gestion devrait être réexaminé afin de s'assurer qu'il est parfaitement conforme au RGPD. Il faut notamment y prévoir qui sera responsable des obligations d'information prévues dans le RGPD vis-à-vis des affiliés et des bénéficiaires, et à qui les grandes lignes de cet accord devront également être mises à disposition. Cette mise à disposition peut être réalisée soit par le biais du règlement de pension, soit en même temps que la communication d'autres informations qui sont mises à la disposition des concernés (voir ci-dessous - point 4).

Nonobstant l'accord que le (les) organisateur(s) et le fonds de pension concluent dans ce cadre, les affiliés et les bénéficiaires pourront toujours, pour l'exercice de leurs droits fondés sur le RGPD (comme notamment le droit d'accès, d'amélioration, d'effacement, d'objection et de limitation), s'adresser tant à l'un qu'à l'autre. Il conviendra dès lors également qu'une partie de leur accord prévoie les suites concrètes données dans cette situation.

En tant que responsables conjoints du traitement, le (les) organisateur(s) et le fonds de pension sont solidairement responsables vis-à-vis des affiliés et des bénéficiaires pour les dommages qu'ils subissent des suites

d'une violation du RGPD (par ex., le dommage causé par une perte de données).

Ils disposent toutefois mutuellement d'un droit de recours pour les dommages qu'ils ont indemnisés mais pour lesquels ils ne sont pas responsables en vertu de leur accord relatif à leurs missions et responsabilités. Dans ce cas, le fonds de pension peut introduire un recours contre le (les) organisateur(s) ou *vice versa*. Il vaut également mieux que ceci soit clairement réglé dans la convention de gestion. Il s'agit d'un point d'attention, en particulier pour les fonds de pension multi-employeurs qui sont ouverts aux entreprises qui n'ont pas de lien économique entre elles ou avec ces fonds.

La question se pose de savoir si cette responsabilité solidaire a également un impact sur les amendes administratives qui peuvent être imposées en cas de non-respect du RGPD et qui peuvent atteindre jusqu'à 20.000.000 EUR ou - pour les entreprises - 4% du chiffre d'affaires annuel (si ce montant est supérieur à 20.000.000 EUR).

Selon nous, la réponse est négative : la responsabilité solidaire s'applique uniquement vis-à-vis des affiliés et bénéficiaires pour les dommages qu'ils subissent dans le cadre du traitement de leurs données à caractère personnel, et non pour les amendes administratives. A notre avis, ces dernières peuvent uniquement être imposées par l'autorité de contrôle (la Commission de la protection de la vie privée - future Autorité de protection des données) à celui qui a commis l'infraction et non au responsable conjoint du traitement qui n'est en aucun cas responsable du fait dommageable.

### 3 Fondements juridiques pour le traitement

Les données à caractère personnel peuvent uniquement être traitées sur la base de l'un des fondements juridiques prévus dans le RGPD. Il s'agit des mêmes fondements juridiques que ceux prévus par la réglementation actuelle, bien que des conditions plus strictes soient désormais imposées pour certains d'entre eux.

#### 3.1 Le consentement comme fondement juridique

C'est notamment le cas pour le consentement comme fondement juridique pour le traitement, tant pour le contenu que pour la manière dont ce consentement doit être donné. Il doit désormais s'agir d'un acte explicite et actif. Un consentement tacite ou implicite ne suffit pas.

De plus, le consentement doit être donné librement pour pouvoir être considéré comme un fondement juridique licite. Dans le cadre de la réglementation actuelle, il existait déjà des discussions sur la question de savoir si un travailleur pouvait réellement donner son consentement, compte tenu de la position de subordination de ce dernier vis-à-vis de son employeur. A cet égard, le Groupe de travail « Article 29 » (G29)<sup>1</sup> a récemment confirmé dans son avis 2/2017 sur le traitement des données au travail que les travailleurs ne peuvent donner leur consentement libre que dans des circonstances exceptionnelles, compte tenu des inégalités inhérentes à ce rapport de force. La Commission de la

<sup>1</sup> Le G29 est un groupe de travail européen indépendant qui traite de sujets relatifs à la protection des données à caractère personnel et de la vie privée. Il a été « créé » par l'article 29 de la Directive Protection des données (directive 95/46/CE) et a été mis en place en 1996. Il est composé de représentants de toutes les autorités nationales de protection des données des Etats-membres de l'UE, du Contrôleur Européen de la Protection des Données et de la Commission européenne. Le G29 dispose d'une mission d'avis mais ses avis jouissent d'une autorité importante du fait de sa composition.

protection de la vie privée adopte une position similaire sur son site internet.

Il convient dès lors de conclure que le consentement ne peut constituer la (seule) base juridique pour le traitement des données à caractère personnel des travailleurs. En outre, le consentement doit à tout moment pouvoir être retiré, ce qui est susceptible d'entraîner de nombreux problèmes pratiques dans l'administration des pensions.

#### 3.2 Exécution du contrat de travail individuel ou d'une convention collective de travail comme fondement juridique

Pour le traitement des données à caractère personnel des (ex-)travailleurs affiliés, il est possible d'invoquer l'exécution du contrat de travail individuel ou d'une CCT applicable comme fondement juridique. Lorsqu'il s'agit d'un régime d'entreprise, le règlement de pension constitue en effet une partie intégrée au contrat de travail individuel. Dans l'hypothèse d'un régime de pension sectoriel, ce règlement constitue un chapitre d'une CCT, via laquelle les dispositions normatives individuelles sont incorporées dans le contrat de travail individuel. Pour l'exécution de ce contrat de travail individuel (en ce compris l'engagement de pension ou le règlement de pension), le traitement des données du (de l'ex-)travailleur affilié est nécessaire.

Ce fondement juridique ne peut cependant pas être utilisé pour le traitement des données des bénéficiaires.

#### 3.3 Respect d'une obligation légale comme fondement juridique

Pour les bénéficiaires, mais aussi pour les affiliés, les obligations légales incombant aux organisateurs et aux fonds de pension sur la base de la loi du 28 avril 2003 relative aux pensions complémentaires (LPC) et/ou la loi du 27 octobre 2006 relative au contrôle des

institutions de retraite professionnelle (LIRP) et leurs arrêtés d'exécution peuvent être invoquées.

Même s'il n'existe aucune obligation d'organiser une pension complémentaire mais que l'employeur ou l'organisateur sectoriel l'organise malgré tout, les dispositions (impératives) de la LPC et de la LIRP s'appliquent. Le(s) organisateur(s) et le fonds de pension sont alors obligés de traiter les données personnelles des (ex)travailleurs affiliés et des bénéficiaires pour exécuter l'engagement de pension conformément aux règles de la LPC et de la LIRP (cf. calcul des réserves et prestations acquises, établissement et communication de la fiche pension annuelle, paiement des prestations de pension, de décès et d'invalidité, communication en cas de sortie, exécution de transferts individuels ou collectifs,...).

En 2011, la Commission de la protection de la vie privée confirmait déjà que, dans le cas d'espèce, le traitement des données à caractère personnel se justifiait par la nécessité de respecter les obligations légales dans le cadre de la gestion des engagements de pension conformément à la LPC et à la LIRP, mais également - pour les affiliés - par le but de respecter le contrat de travail. Etant donné que le RGPD n'a pas apporté de modifications à ces fondements juridiques, nous partons du principe que ce point de vue peut toujours être suivi.

## 4 Elargissement du devoir d'information

### 4.1 Informations complémentaires à fournir

Selon les règles actuelles, le(s) organisateur(s) ou le fonds de pension doivent déjà fournir des informations spécifiques relatives au traitement des données. Il s'agit entre autres des finalités pour lesquelles les données sont traitées,

quelles sont les données traitées, à qui ces données sont communiquées (par exemple des prestataires de services externes impliqués dans l'administration des pensions), le droit d'accès, de rectification, etc.

Actuellement, ces informations sont, la plupart du temps, communiquées aux affiliés et aux bénéficiaires via leur contrat de travail individuel ou un avenant à celui-ci, via la CCT sectorielle applicable, via le règlement de pension, via la fiche de pension annuelle ou via la communication relative aux paiements.

Le RGPD a élargi ce devoir d'information. Les informations complémentaires qui doivent être communiquées sont entre autres : le fondement juridique du traitement des données, la durée de conservation des données, la possibilité de retirer à tout moment son consentement (si le consentement est (un des) le fondement(s) juridique(s)), le droit d'introduire une réclamation à la Commission de la protection de la vie privée, l'envoi ou non des données en-dehors de l'Europe (par exemple, si une partie de l'administration des pensions est réalisée par un prestataire de services externe non-européen) et les garanties particulières à cet égard, etc.

En tant que responsables conjoints du traitement, l'(/les) organisateur(s) et le fonds de pension devront définir dans leur accord qui fournira cette information.

### 4.2 Egalement aux bénéficiaires?

Pour cette obligation d'information, le RGPD établit une distinction selon que les données ont été ou non collectées auprès de la personne concernée. En cas de réponse négative, il est encore éventuellement possible d'invoquer une exception : si la communication d'information semble impossible ou réclame des efforts trop disproportionnés, elle ne doit pas être réalisée. La question se pose de savoir si l'(/les) organisateur(s) et /ou le fonds de pension peuvent s'appuyer sur cette exception.

Dans ce contexte nous pensons qu'il est préférable de réaliser une distinction entre les bénéficiaires potentiels, pour lesquels l' (les) organisateur(s) et le fonds de pension traitent d'ores et déjà les données, et les bénéficiaires effectifs. Nous pensons ici aux partenaires et aux enfants des (ex)travailleurs affiliés, pour lesquels les noms et dates de naissance sont conservés dans le cadre de l'administration des pensions. Aussi longtemps que le travailleur affilié n'est pas décédé, ceux-ci sont des bénéficiaires potentiels sur base de l'ordre des bénéficiaires standard du règlement de pension ou, le cas échéant, sur base d'un formulaire de désignation des bénéficiaires, mais ils n'ont pas encore droit à la moindre prestation de décès et ne sont donc pas encore des bénéficiaires effectifs.

Dans un avis de 2011, la Commission de la protection de la vie privée estimait que les données de ces bénéficiaires potentiels étaient uniquement enregistrées par le biais de l'affilié et que ces données « appartenaient » donc en réalité à l'affilié. Selon la Commission de la protection de la vie privée, en cas d'enregistrement indirect de ce type, l'affilié pouvait être mandaté pour informer les membres de sa famille (les bénéficiaires potentiels) sur le traitement de leur donnée à caractère personnel.

Sur la base de l'exception susmentionnée dans le RGPD et de l'avis de la Commission de la vie privée, il est possible de défendre que les bénéficiaires devront être informés par le fonds de pension du traitement des données uniquement lorsqu'ils pourront effectivement prétendre à une prestation du fonds de pension, et que, dans ce cadre, ils transféreront directement leurs données à caractère personnel au fonds de pension.

## 5 Obligation de déclaration remplacée par une obligation de documentation

### 5.1 Registre des activités de traitement

Selon les règles actuelles, il existe une obligation de déclaration à la Commission de la protection de la vie privée du traitement (partiellement) automatisé.

Avec le RGPD, cette obligation de déclaration disparaît et est remplacée par une obligation de documentation. Celle-ci implique que tant le responsable du traitement que le sous-traitant doivent tenir un registre des activités de traitement.

### 5.2 Traitement des données non occasionnel

Il existe une exception à cette règle. Les entreprises ou organisations qui comptent moins de 250 employés ne doivent tenir aucun registre, sauf si le traitement est susceptible de comporter un risque pour les droits et les libertés des personnes concernées, si des données sensibles sont traitées ou si le traitement n'est pas occasionnel.

Nonobstant le fait que le RGPD ne soit pas totalement clair sur l'étendue de la notion d'« un traitement qui n'est pas occasionnel », il nous semble en tout état de cause difficile d'argumenter que le traitement des données dans le cadre de la gestion et l'exécution des règlements de pension complémentaire est occasionnel. Ceci d'autant plus que ce sont généralement des données sensibles qui sont traitées (de manière limitée), comme, par exemple les données relatives à la maladie et à l'invalidité dans le cadre d'une couverture invalidité.

Dans ce contexte, il faut également relever que la Commission de la protection de la vie privée, dans sa recommandation 06/2017 du

14.06.2017 relative au registre des activités de traitement, a expressément précisé que la gestion du personnel ne peut pas être considérée comme un traitement occasionnel.

Selon nous, le registre s'avérera donc être un instrument au moins nécessaire, si pas utile, dans le cadre de la mise en œuvre du RGPD.

## 6 Délégué à la protection des données (DPD)

Dans le secteur privé, en règle générale, aucun agent pour la protection des données ou *Délégué à la Protection des Données* (DPD) (Data Protection Officer) ne doit être nommé à condition que les données à caractère personnel ne soient traitées qu'à titre d'activité accessoire.

La question se pose de savoir si le traitement de données par le fonds de pension peut être qualifié d'activité accessoire.

Si l'(les) organisateur(s) a (ont) déjà nommé un DPD, cela ne posera sans doute aucun problème. Le même DPD peut en effet également assumer cette fonction pour le fonds de pension. Lorsque l' (les) organisateurs n'a (ont) pas non plus de DPD, la fonction de conseiller en sécurité (que tout fonds de pension doit avoir instituée dans le cadre des normes minimales de sécurité pour la sécurité de l'information imposées par la BCSS) et de DPD peuvent éventuellement être combinées.

Sur le même point, nous nous référons à la recommandation 04/2017 sur ce sujet du 24.05.2017 de la Commission de la protection de la vie privée. Dans cette recommandation, la Commission de la protection de la vie privée n'exclut pas la combinaison des fonctions de DPD et de conseiller en sécurité. C'est au responsable du traitement ou au sous-traitant de déterminer si ce cumul est licite. Par contre, la Commission de la protection de la vie privée indique qu'il n'y a pas de transfert automatique ou systématique de la fonction de conseiller en

sécurité vers la fonction de DPD et qu'une éventuelle combinaison doit toujours être examinée *in concreto*. Dans tous les cas, le DPD doit disposer des connaissances spécialisées du droit et des pratiques en matière de protection des données.

## 7 Documents à vérifier

En guise de conclusion, nous résumons brièvement les documents qui, dans le cadre de la mise en œuvre du RGPD, devraient idéalement être passés en revue par le(s) organisateur(s) et/ou les fonds de pension:

- L'éventuelle clause relative au traitement des données dans le cadre du plan de pension complémentaire reprise dans le contrat de travail ou l'annexe à celui-ci;
- La clause dans la convention de gestion concernant le partage conventionnel des tâches et des responsabilités entre le(s) organisateur(s) et le fonds de pension ;
- L'(éventuelle) clause relative au traitement des données reprise sur la fiche de pension annuelle et sur les autres communications qui sont faites aux affiliés et/ou aux bénéficiaires.
- L'(éventuelle) clause relative au traitement des données reprise dans le formulaire de désignation des bénéficiaires;
- Les contrats conclus avec des prestataires de service externes qui reçoivent et/ou traitent des données pour le(s) organisateur(s) et/ ou le fonds de pension ; en vertu du RGPD quelques dispositions supplémentaires devront être prévues



**Claeys & Engels vous informe**

A la fin de cette année, nous organiserons un workshop, dans lequel nous approfondirons la mise en œuvre concrète du RGPD dans le cadre de la gestion des plans de pension complémentaire. Vous recevrez une invitation à participer à cet évènement dans les semaines à venir.



**Bruxelles**

280, Bd. du Souverain  
1160 Bruxelles  
Tel.: 02 761 46 00  
Fax: 02 761 47 00

**Liège**

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

**Anvers**

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

**Gand**

F. Lousbergkaai 103  
bus 4-5  
9000 Gand  
Tel.: 09 261 50 00  
Fax: 09 261 55 00

**Courtrai**

Ring Bedrijvenpark  
Brugsesteenweg 255  
8500 Courtrai  
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.* ●