CODE DE CONDUITE CONCERNANT LE TRAITEMENT ET LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

1 Objectif

Le présent code de conduite fournit toutes les informations et instructions pertinentes pour toute personne qui, dans l'exercice de sa fonction au sein d'Ogeo Fund (ci-après, l'« IRP ») traite des données à caractère personnel dans le cadre des obligations de pension légale (premier pilier) dont la gestion et l'exécution ont été confiées à Ogeo Fund.

Le présent code de conduite est rédigé afin d'assurer le respect par l'IRP, qui est dans certains cas considéré comme un responsable de traitement distinct des Entreprises d'affiliation et dans d'autres comme leur sous-traitant, du Règlement européen 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données, ou « RGPD »), ainsi que la législation et la réglementation belge applicable en matière de protection des données.

Le présent code de conduite ne vise pas à fournir une protection plus importante que celle requise par la législation applicable en matière de protection des données.

2 Champ d'application

Le présent code de conduite est applicable au traitement des données à caractère personnel dans le cadre de la gestion et l'exécution des obligations de pension légale (premier pilier) des affiliés d'Ogeo Fund.

Le présent code de conduite a été rédigé pour toute personne qui, dans l'exercice de sa fonction au sein de l'IRP, traite des données à caractère personnel dans le cadre de la gestion et l'exécution des obligations de pension légale (premier pilier), dont notamment :

- les membres actuels et futurs du personnel de l'IRP qui réalisent ce traitement de données à caractère personnel ;
- les administrateurs et membres des autres organes (opérationnels) de l'IRP ;
- le cas échéant, les membres des comités de surveillance et des autres comités d'avis constitués dans le cadre de la gestion et de l'exécution des obligations de pension légale (premier pilier).

Elle complète mais ne remplace pas les obligations relatives à la protection des données à caractère personnel qui s'appliquent à eux en vertu de la note de politique d'intégrité mais également des dispositions suivantes, internes à l'IRP :

- code de déontologie ;
- guide de bonne gouvernance.

3 Définitions

Le RGPD et le présent Code de conduite utilisent des termes spécifiques. Voici les définitions des termes les plus importants :

- **« Affiliés »** signifie les membres du personnel statutaires de l'entreprise d'affiliation dont la gestion des engagements de pension du 1er pilier restés à sa charge après son affiliation au SFP, est confiée à Ogeo Fund ;
- **« Bénéficiaires »** signifie les personnes qui, conformément à la couverture décès prévue dans les obligations de pension légale (premier pilier), ont droit à une prestation en cas de décès d'un affilié. Dans ce cadre, une distinction est faite entre les bénéficiaires potentiels et les bénéficiaires effectifs ; Les **« bénéficiaires potentiels »** sont les personnes qui, en cas de décès de l'Affilié, auront droit à une prestation décès (par exemple : le partenaire ou les enfants) et qui sont indirectement enregistrées par l'IRP et/ou l'entreprise d'affiliation dans le cadre de l'enregistrement de l'Affilié. Les **« bénéficiaires effectifs »** sont les personnes qui, légalement, ont effectivement droit à une prestation en cas de décès. Le concept de « bénéficiaire » signifie également les personnes qui perçoivent régulièrement une prestation de l'IRP. Sont dans ce dernier cas visés les rentiers et les éventuels bénéficiaires de la réversibilité d'une rente ;
- **« Entreprise d'affiliation »** signifie l'entité publique qui a confié à l'IRP la gestion et l'exécution des obligations en matière de pension légale (premier pilier) ;
- **«L'Espace Economique Européen** («**EEE**»)**»** qui comprend actuellement les pays suivants: l'Allemagne, l'Autriche, la Belgique, la Bulgarie, la Croatie, Chypre, le Danemark, l'Espagne, l'Estonie, la Finlande, la France, la Grèce, la Hongrie, l'Irlande, l'Italie, l'Islande, la Lettonie, le Liechtenstein, la Lituanie, le Luxembourg, Malte, la Norvège, les Pays-Bas, la Pologne, le Portugal, la République Tchèque, la Roumanie, le Royaume-Uni, la Slovénie, la Slovaquie et la Suède;
- **«Données à caractère personnel»** signifie toute information se rapportant à une personne physique identifiée ou identifiable (« la personne concernée »). Dans le cadre de la gestion et de l'exécution des obligations de pension légale (premier pilier) par OGEO FUND, il s'agit des données à caractère personnel des affiliés et des bénéficiaires au sens des obligations de pension légale (premier pilier) ;
- «**Données particulières**» signifie des données à caractère personnel qui révèlent, d'une personne:
  - son origine raciale ou ethnique;
  - ses opinions politiques;
  - ses croyances religieuses ou philosophiques;
  - son appartenance syndicale;
  - des données concernant sa santé ou sa vie sexuelle;
  - des données relatives à des condamnations pénales et à des infractions ou des mesures de sûreté connexes ;
- **« IRP »** signifie ici l'OFP Ogeo Fund, institution de retraite professionnelle autorisée par l'Autorité des Services et Marchés Financiers (FSMA) et inscrite sous le numéro d'identification 50570 ;

- **« Législation et règlementation en matière de protection des données »** signifie le Règlement européen 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données, ou RGPD), ainsi que la législation et la réglementation belge et européenne applicable en matière de protection des données ;
- **«Responsable du traitement»** signifie une personne ou organisation qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel. Dans le cadre de la gestion et de l'exécution des obligations de pension légale (premier pilier), l'IRP et l'entreprise d'affiliation sont chacune responsables du traitement distincts ;.
- **« Sous-traitant »** signifie la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte d'un(de) responsable(s) du traitement ;
- **«Personne concernée»** signifie toute personne qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ;
- **«Traitement»** est défini comme 'toute opération ou tout ensemble d'opérations effectuées, ou non, à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction'. Ceci signifie que le terme 'traitement' a une étendue très large ;
- **«Utilisateurs autorisés »** signifie les personnes qui, dans le cadre de l'exercice de leur fonction au sein de l'IRP ou de l'entreprise d'affiliation sont autorisées, dans le cadre de la gestion et l'exécution des obligations de pension légale (premier pilier), à traiter des données à caractère personnel sur instruction de l'IRP et/ou de l'entreprise d'affiliation. Il peut s'agir, entre autres, des membres du personnel de l'entreprise d'affiliation, des membres du personnel de l'IRP, des administrateurs de l'IRP, membres des comités de surveillance et des autres comités d'avis constitués dans le cadre de la gestion et de l'exécution des obligations de pension légale (premier pilier) ;
- **«Violation de données à caractère personnel»** est définie comme 'une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

4 Principes pour traiter les données à caractère personnel

L'IRP respecte la vie privée des affiliés et bénéficiaires dont les données à caractère personnel sont traitées dans le cadre de la gestion et l'exécution des obligations de pension légale (premier pilier), et s'engage à protéger leurs données à caractère personnel en conformité avec le RGPD et la législation et règlementation en matière de protection des données.

L'IRP respectera, entre autres, les principes suivants lors des traitements de données à caractère personnel dans le cadre de la gestion et de l'exécution des obligations de pension légale (premier pilier):

- Traitement licite de données et finalités déterminées : l'IRP traite les données à caractère personnel pour les finalités déterminées licites déterminées au point 7.

- Limitation des finalités : l'IRP ne traite pas les données à caractère personnel pour d'autres finalités.

- Minimisation du traitement des données : l'IRP limite le traitement des données à caractère personnel à ce qui est nécessaire dans le cadre des finalités susmentionnées.

- Exactitude des données à caractère personnel : l'IRP prend toutes les mesures raisonnables pour veiller à ce que les données à caractère personnel soient exactes et qu'elles soient rectifiées et/ou effacées sans tarder si elles n'apparaissent plus exactes.

- Limitation du traitement et de la conservation : l'IRP ne traitera et ne conservera pas les données à caractère personnel plus que nécessaire pour les finalités susmentionnées.

- Mesures de sécurité : l'IRP prend les mesures techniques et/ou organisationnelles nécessaires/adéquates pour la sécurité des données à caractère personnel des affiliés et des bénéficiaires et pour éviter une violation et/ou une fuite informatique (comme un accès non autorisé, le traitement illicite et non autorisé ou la perte, la destruction ou les dégâts d'origine accidentelle des données à caractère personnel). Ces mesures sont régulièrement évaluées et si nécessaire actualisées. En cas de violation ou de fuite informatique, comme décrit ci-dessous au point 14, l'IRP prend les mesures nécessaires/adéquates pour en constater l'étendue et les conséquences, y mettre fin le plus vite possible et, le cas échéant, limiter son impact pour les affiliés et/ou bénéficiaires.

5 Délégué à la protection des données ('Data Protection Officer')

L'IRP a désigné un délégué à la protection des données qui peut être contacté de la manière suivante: Jean-François Henrotte, Boulevard d'Avroy, 280 à 4000 LIEGE; Tél : 04/2220115; e-mail : privacy@ogeofund.be.

Ce délégué à la protection des données est compétent :

- pour informer et conseiller l'IRP, ainsi que les membres du personnel de l'Entreprise d'affiliation, les administrateurs de l'IRP, les membres des autres organes (opérationnels) de l'IRP, les membres des autres comités d'avis constitués dans le cadre de la gestion et de l'exécution des obligations de pension légale (premier pilier), quant aux obligations qui leur incombent en vertu de la législation et règlementation en matière de protection des données.

- pour contrôler le respect de la législation et règlementation en matière de protection des données et de la politique de traitement et de protection des données dans le cadre de la gestion et de l'exécution des obligations de pension légale (premier pilier) tels que repris dans le présent code de conduite, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant.

- pour dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données (voir point 9) et d'en vérifier l'exécution.

- pour coopérer avec l'Autorité de Protection des Données.

- pour faire office de point de contact pour:

- les affiliés et les bénéficiaires, qui peuvent contacter le délégué à la protection des données pour toutes les questions liées au traitement de leurs données à caractère personnel et à l'exercice de leurs droits.
- les utilisateurs autorisés, affiliés ou bénéficiaires ou toute autre personne qui constatent un incident ou une violation en lien avec le traitement des données à caractère personnel dans le cadre de la gestion et de l'exécution des obligations de pension légale (premier pilier) et qui doivent entre autres en informer le délégué à la protection des données (voir point 15).
- l'Autorité de Protection des Données en ce qui concerne les questions liées au traitement, en ce compris la consultation préalable, et pour la consulter, le cas échéant, en ce qui concerne toute autre question.

- pour tenir dûment compte du risque associé aux opérations de traitement, compte tenu de la nature, de la portée, du contexte et des finalités du traitement.

- pour toute autre mission ou tâche, dans la mesure où celles-ci n'entraînent pas de conflit d'intérêts.

Le délégué à la protection des données est soumis au secret professionnel ou à une obligation de confidentialité en ce qui concerne l'exercice de ses missions.

6 Catégories de données traitées

6.1 Affiliés

Les données à caractère personnel des affiliés comportent les données suivantes, limitées aux données spécifiques qui sont nécessaires pour la gestion et l'exécution des obligations de pension légale (premier pilier) concernées :

- données de contact (nom, prénom(s), adresse, numéro de téléphone, adresse e-mail, langue etc.) ;
- données relatives à l'état civil (date et lieu de naissance, numéro de registre national, état civil, domicile fiscal, sexe, composition familiale, nom, date de naissance, adresse et/ou sexe de votre partenaire et/ou de vos enfants et/ou de vos bénéficiaires désignés,
- données relatives à l'emploi auprès d'une Entreprises d'affiliation (années de service, fonction, régime d'emploi, périodes de suspension du contrat de travail, informations relative à des incapacités de travail, etc.) ;
- données financières (numéro de compte bancaire, salaires, avantages, bonus, etc.).
- données particulières (données relatives à la santé, sexe du partenaire légal et/ou de vos enfants et/ou de vos bénéficiaires désignés).

6.2 Bénéficiaires

Les données à caractère personnel des bénéficiaires comportent les données suivantes, limitées aux données spécifiques qui sont nécessaires pour la gestion et l'exécution des obligations de pension légale (premier pilier) concernées :

- données de contact : (nom, prénom(s), adresse, numéro de téléphone ; adresse e-mail ; langue etc.).

- données relatives à l'état civil (date et lieu de naissance ; numéro de registre national ; état civil ; domicile fiscal ; sexe ; composition familiale ; nom, date de naissance, adresse et/ou sexe du partenaire et/ou des enfants ;...).
- données financières (numéro de compte bancaire),
- données particulières (sexe du partenaire légal et/ou des bénéficiaires).

6.3 Données à caractère personnel particulières

L'IRP peut, lorsque cela est nécessaire pour la gestion et la mise en œuvre des obligations de pension légale (premier pilier), traiter des données à caractère personnel particulières, en ce compris des données indirectement liées à la santé (par exemple, les périodes d'incapacité de travail, l'enregistrement d'accident, ... dans le contexte des couvertures de risque prévues par des obligations de pension légale (premier pilier)) et les données relatives au sexe du partenaire légal et des bénéficiaires.

7 Finalités du traitement de données à caractère personnel

L'IRP traite les données à caractère personnel uniquement pour finalités légitimes liées **à la gestion et l'exécution des obligations de pension légale (premier pilier)**. Ces finalités sont les suivantes :

- l'administration des pensions, en ce compris la gestion administrative de l'affiliation ;
- le calcul des provisions techniques ;
- le calcul et le paiement des prestations conformément aux notes techniques et aux plans de financement (rente, rente de survivant, rente d'orphelin, rente d'invalidité) ;
- le calcul des contributions pour financer des obligations de pension légale (premier pilier) ;
- la rédaction de la correspondance ;
- la réalisation de transferts collectifs et individuels ;
- la gestion financière et comptable des obligations de pension légale (premier pilier) ;
- pour la communication avec les autorités de contrôle et notamment le reporting à la FSMA, à la BNB et aux autres autorités compétentes lorsque cela est indiqué, en ce compris les échanges avec ces autorités ;
- le reporting au Service Fédéral des Pensions (Cadastre des Pensions), en ce compris les échanges avec ce service public ;
- le respect des obligations légales imposées par la loi du 27 octobre 2006 relative au contrôle des institutions de retraite professionnelle (la « LIRP) et ses arrêtés d'exécution.

Les données à caractère personnel ne sont pas traitées par ou pour le compte de l'IRP d'une manière qui est incompatible avec ces finalités.

8 Sécurité/confidentialité

L'IRP s'engage à adopter les mesures techniques, physiques et organisationnelles nécessaires/adéquates pour protéger les données à caractère personnel contre l'accès non autorisé, le traitement illicite, la perte ou le dommage accidentels, et la destruction non autorisée.

8.1 Sécurité de l'équipement et de l'information

Toutes les données à caractère personnel électroniques détenues par l'IRP sont conservées dans des systèmes protégés par des architectures de réseau sécurisé mis à jour, qui contiennent des firewalls et des périphériques de détection d'intrusion, afin d'empêcher les accès non autorisés aux données à caractère personnel par des tiers. Il existe un "back up" des données sauvées sur les serveurs de manière à éviter les conséquences d'un effacement, d'une destruction ou d'une perte accidentels. Les serveurs se trouvent dans des installations avec un haut degré de sécurité.

8.2 Sécurité d'accès

L'importance de la sécurité de toutes les données à caractère personnel liées aux affiliés et aux bénéficiaires qui sont collectées, conservées et traitées dans le cadre de la gestion et de l'exécution des obligations de pension légale (premier pilier) est une préoccupation majeure pour l'IRP. L'IRP s'engage à protéger l'intégrité des informations personnelles et à empêcher l'accès non autorisé à celles-ci.

Des mesures sont conçues et prévues pour empêcher la corruption de données, pour bloquer l'accès inconnu et non autorisé à notre système informatique et à nos informations, et pour fournir une protection raisonnable des données à caractère personnel que l'IRP possède. Tous les dossiers sont conservés confidentiellement dans des classeurs ou des pièces sécurisées et verrouillées. L'accès aux bases de données informatisées est contrôlé par une séquence login et requiert que les utilisateurs autorisés s'identifient eux-mêmes et fournissent un mot de passe avant que l'accès ne soit accordé. Les utilisateurs autorisés sont limités aux données nécessaires pour exercer leur fonction dans le cadre de la gestion et de l'exécution des obligations de pension légale (premier pilier). Les caractéristiques de sécurité des softwares et des procédures développées sont utilisées pour protéger les informations personnelles de perte, d'abus, et d'accès non autorisé, de divulgation, d'altération, et de destruction.

8.3 Formation

L'IRP veillera à l'organisation de sessions de formation nécessaires pour les utilisateurs autorisés à propos notamment : des finalités licites, énumérées et prévues pour le traitement de données à caractère personnel, du besoin de protéger et de garder l'information exacte et à jour, et du besoin de maintenir la confidentialité des données auxquelles les utilisateurs autorisés ont accès.

Les utilisateurs autorisés s'engageront à respecter la confidentialité des données à caractère personnel et à se conformer au présent code de conduite. L'IRP prendra les mesures nécessaires conformément à la législation et règlementation en matière de protection des données, s'il est accédé à des données à caractère personnel, ou si elles sont traitées ou utilisées de quelque manière qui ne soit pas conforme aux exigences du présent Code de conduite.

8.4 Instructions générales

Tous les utilisateurs autorisés sont tenus par le présent Code de conduite de faire le nécessaire pour respecter les règles établies afin que l'IRP, en tant que responsable du traitement distinct, respecte la législation et règlementation en matière de protection des données. L'IRP s'engage à protéger les données à caractère personnel des affiliés et bénéficiaires lors de l'utilisation ou du traitement de celles-

ci. C'est pourquoi les utilisateurs autorisés doivent reconnaître l'importance d'un traitement correct et licite des données à caractère personnel, et qu'ils doivent gérer les données à caractère personnel avec le plus grand soin et en stricte conformité avec le présent Code de conduite.

En outre, les utilisateurs autorisés doivent être informés que la non-conformité au présent Code de conduite peut mener à de graves conséquences négatives sur la vie privée des affiliés et bénéficiaires, ainsi que pour l'IRP (entre autres, les amendes élevées imposées par l'Autorité de Protection des Données, les atteintes à la réputation, ...).

Au plus tard au moment où les utilisateurs autorisés reçoivent pour la première fois accès aux données à caractère personnel et l'autorisation de traiter ces données à caractère personnel conformément aux instructions de l'IRP, ils reçoivent le présent Code de conduite qui leur est expliqué. Ils peuvent uniquement avoir accès aux données à caractère personnel et être autorisés à traiter les données à caractère personnel après qu'ils se sont engagés à respecter le présent Code de conduite.

9 Analyse d'Impact relative à la protection des données

Si une activité de traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des affiliés et bénéficiaires, l'IRP effectuera, conformément à la législation et règlementation en matière de protection des données une analyse d'impact relative à la protection des données afin d'évaluer, en particulier, l'origine, la nature, la particularité et la gravité de ce risque.

Il sera tenu compte du résultat de cette analyse pour déterminer les mesures appropriées à prendre. S'il ressort de l'analyse d'impact relative à la protection des données que les opérations de traitement des données comportent un risque élevé que le responsable du traitement ne peut atténuer en prenant des mesures appropriées compte tenu des techniques disponibles et des coûts liés à leur mise en œuvre, il convient que l'Autorité de Protection des Données soit consultée avant que le traitement n'ait lieu.

Même lorsqu'une analyse d'impact relative à la protection des données n'est pas requise sur la base de la législation et règlementation en matière de protection des données, l'IRP peut néanmoins décider de réaliser une telle analyse d'impact relative à la protection des données préalablement à la réalisation d'une activité de traitement.

Dans le cadre de la mise en œuvre du RGPD, l'IRP a réalisé un *mapping* et un audit étendus des activités de traitement dans le cadre de la gestion et de l'exécution des obligations de pension légale (premier pilier). Ces *mapping* et audit constituent une analyse d'impact relative à la protection des données des activités de traitement actuelles dans le cadre de la gestion et de l'exécution des obligations de pension légale (premier pilier).

10 Diffusion de l'information relative au traitement des données à caractère personnel

10.1 Affiliés

Au moment de l'affiliation aux obligations de pension légale (premier pilier), l'entreprise d'affiliation remet, pour compte de l'IRP, à l'affilié, via une lettre, les informations légales requises concernant le traitement des données au sein de l'IRP, dont notamment :

- les coordonnées de l'IRP et de l'entreprise d'affiliation ;
- les finalités de traitement pour lesquelles les données à caractère personnel sont traitées, à savoir la gestion et l'exécution des obligations de pension légale (premier pilier) ;
- les bases légales du traitement, la loi du 26 octobre 2007 relative au contrôle des institutions de retraite professionnelle (LIRP) et/ou ses arrêtés d'exécution et des obligations de pension légale (premier pilier) ;
- les tiers possibles qui sont impliqués ou pourraient être impliqués dans l'exécution des obligations de pension légale (premier pilier) et qui dans ce cadre peuvent traiter des données à caractère personnel (sous-traitant) et/ou recevoir des données à caractère personnel (destinataires) ;
- les règles concernant la durée de la période dans laquelle les données à caractère personnel seront traitées et/ou conservées ;
- la possibilité d'introduire une plainte auprès de l'Autorité de Protection des Données ;
- les coordonnées du délégué à la protection des données ;
- les droits de l'affilié relatifs à l'accès, la rectification, l'effacement, la restriction et la portabilité des données à caractère personnel.

10.2 Bénéficiaires

Bénéficiaires potentiels

Concernant l'obtention des données relatives aux bénéficiaires potentiels découlant d'une obligation légale, l'OFP Ogeo Fund est dispensé de porter les présentes informations à leur égard.

Cependant, l'affilié peut naturellement lui communiquer la présente lettre s'il le souhaite.

Bénéficiaire Effectifs

Lorsqu'un bénéficiaire bénéficie d'une prestation en cas de décès en vertu des obligations de pension légale (premier pilier), l'IRP communique à ce bénéficiaire effectif les informations légales requises concernant le traitement des données, en même temps que la communication relative à la couverture décès, dont notamment :

- les coordonnées de l'IRP et de l'entreprise d'affiliation ;
- les finalités de traitement pour lesquelles les données à caractère personnel sont traitées, à savoir la gestion et l'exécution des obligations de pension légale (premier pilier) (couverture décès) ;
- les bases légales du traitement, à savoir la loi du 26 octobre 2007 relative au contrôle des institutions de retraite professionnelle (LIRP) et/ou leurs arrêtés d'exécution respectifs et des obligations de pension légale (premier pilier) ;
- les tiers possibles qui sont impliqués ou pourraient être impliqués dans l'exécution des obligations de pension légale (premier pilier) et qui dans ce cadre peuvent traiter des données à caractère personnel (sous-traitant) et/ou recevoir des données à caractère personnel (destinataires) ;
- les règles concernant la durée de la période dans laquelle les données à caractère personnel seront traitées et/ou conservées ;
- la possibilité d'introduire une plainte auprès de l'Autorité de Protection des Données ;
- les coordonnées du délégué à la protection des données ;
- les droits du bénéficiaire relatifs à l'accès, la rectification, l'effacement, la restriction et la portabilité des données à caractère personnel.

11 Principes généraux sur les droits des personnes concernées

L'IRP facilitera l'exercice des droits susmentionnés des affiliés et des bénéficiaires concernant le traitement des données à caractère personnel dans le cadre des obligations de pension légale (premier pilier). Elle ne refusera pas de donner suite à la demande de l'affilié ou du bénéficiaire d'exercer ses droits, à moins qu'elle puisse démontrer qu'elle n'est pas en mesure d'identifier l'affilié ou le bénéficiaire. Si l'IRP a des doutes raisonnables quant à l'identité de la personne physique présentant la demande visée dans ces clauses, il peut demander que lui soient fournies des informations supplémentaires nécessaires pour confirmer l'identité de la personne concernée.

L'IRP transmet les éventuelles demandes à l'Entreprise d'affiliation qui les traite pour le compte de l'IRP. L'Entreprise d'affiliation fournit à l'affilié ou au bénéficiaire des informations sur les mesures prises à la suite d'une demande formulée en application de ses droits, dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande. Au besoin, ce délai peut être prolongé de deux mois, compte tenu de la complexité et du nombre de demandes.

Les mesures ci-après (communication d'information, correction ou effacement de données à caractère personnel, portabilité des données à caractère personnel, etc.) sont gratuites pour l'affilié ou le bénéficiaire demandeur. Lorsque les demandes de l'affilié ou du bénéficiaire sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif, l'IRP ou l'Entreprise d'affiliation peut soit (a) exiger le paiement de frais raisonnables qui tiennent compte des coûts administratifs supportés pour fournir les informations, procéder aux communications ou prendre les mesures demandées; ou (b) refuser de donner suite à ces demandes.

11.1 Demande d'accès de la personne concerné

Tout affilié ou bénéficiaire a le droit de faire une demande d'accès. Si un affilié ou un bénéficiaire exerce ce droit, l'IRP est tenue par la loi de lui fournir des informations à ce sujet, en ce compris :

- donner une description et une copie des données à caractère personnel ;
- informer la personne concernée des raisons pour lesquelles l'IRP traite ces données.

11.2 Rectification, limitation ou effacement

Si des données à caractère personnel sont inexactes ou incomplètes, l'affilié ou le bénéficiaire peut demander à ce que ces données soient corrigées.

Dans certaines circonstances, l'affilié ou le bénéficiaire peut, conformément à la législation et règlementation en matière de protection des données demander l'effacement d'une donnée à caractère personnel le/la concernant, entre autres si la donnée à caractère personnel n'est plus nécessaire pour les finalités pour lesquelles elle avait été collectée ou traitée, ou si l'affilié ou le bénéficiaire s'oppose au traitement pour des raisons légitimes. Dans certains cas, l'IRP peut cependant refuser d'effacer ces données, par exemple au motif qu'elles sont nécessaires pour l'introduction, la mise en œuvre ou la preuve d'un droit en justice.

Dans certaines circonstances, par exemple lorsque l'exactitude de la donnée est contestée ou lorsque l'affilié ou le bénéficiaire s'est opposé au traitement, il peut demander que le traitement de sa donnée à caractère personnel soit limité, ce qui signifie que la donnée à caractère personnel n'est pas effacée le

temps que la contestation soit traitée, mais ne peut être utilisée. La donnée en question est marquée et cela est clairement indiqué dans le dossier.

11.3 Opposition au traitement et au transfert de données à caractère personnel

Dans certaines circonstances, l'affilié ou le bénéficiaire a également le droit de s'opposer au traitement de ses données à caractère personnel. L'IRP ne fait pas droit à de telles objections si des motifs légitimes et impérieux qui prévalent sur les intérêts, droits et libertés de l'affilié ou du bénéficiaire peuvent être invoqués, ou si ces données sont nécessaires pour soutenir une action en justice.

11.4 Portabilité des données

Lorsque cela est nécessaire et dans la mesure où cela est applicable, l'affilié ou le bénéficiaire peut demander de recevoir certaines données à caractère personnel qu'il/elle a fournies à l'IRP ou aux Entreprises d'affiliation dans le cadre de la gestion et de l'exécution des obligations de pension légale (premier pilier), et de transférer ces données vers un autre responsable du traitement. Lorsque cela est techniquement possible, l'affilié ou le bénéficiaire peut demander aux Entreprises d'affiliation de transférer directement ces données vers un autre responsable du traitement. Ce droit ne peut cependant pas porter atteinte aux droits et libertés des autres.

11.5 Plainte

Si l'affilié ou le bénéficiaire a des réclamations concernant le traitement de ses données à caractère personnel, il peut en faire part au délégué à la protection des données (voir point 5 pour les coordonnées de contact).

L'affilié ou le bénéficiaire peut également déposer plainte auprès de l'Autorité de Protection des Données.

12 Conservation de données à caractère personnel

L'IRP ne conservera les données à caractère personnel que le temps nécessaire pour les finalités décrites dans le présent Code de conduite, c'est-à-dire tant que l'IRP et/ou l'entreprise d'affiliation ont une obligation légale ou peuvent être tenues légalement responsables dans le cadre de la gestion et l'exécution des obligations de pension légale (premier pilier) pour lesquelles l'utilisation des données à caractère personnel peut être pertinente, compte tenu des délais de prescription légale applicables.

L'IRP s'assure que les données à caractère personnel sont effacées après l'expiration des délais de conservation susmentionnés et prend les mesures nécessaires afin d'assurer que les données à caractère personnel sont également effacées auprès des sous-traitants qui disposent de ces données. L'effacement se produit sans retard déraisonnable.

13 Transfert vers des tiers

Les données à caractère personnel peuvent être communiquées à des tiers si la diffusion de celles-ci entre dans l'une des finalités de traitement sur lesquelles le traitement des données est basé, et si la diffusion est jugée licite et loyale pour les affiliés et les bénéficiaires.

L'IRP peut également diffuser des données à caractère personnel :

- si l'affilié / le bénéficiaire donnent leur consentement;
- si cela est légalement exigé; et
- en lien avec des enquêtes pénales ou d'autres enquêtes menées par les autorités.

Dans le cadre de la gestion et de l'exécution des obligations de pension légale (premier pilier), les données à caractère personnel peuvent être communiquées, notamment via la Banque Carrefour de la Sécurité Sociale, à des tiers par l'IRP, et même sous-traitées par ces tiers, tels que :

- les autorités et/ou les institutions gouvernementales,
- un administrateur des pensions ;
- un actuaire ;
- un auditeur interne ;
- un commissaire agréé ;
- un compliance officer ;
- un conseiller juridique ;
- un consultant financier;
- un autre professionnel et/ou prestataire de services/conseiller spécialisé ;
- un liquidateur ;
- un secrétariat social ;
- un délégué pour la protection des données (DPO) ;
- des entreprises IT ou des prestataires de services pour des programmes software concernant l'administration de pensions et le stockage de données électroniques (serveurs, etc.) ;
- l'administration de la sécurité sociale ;
- l'administration fiscale ;
- le Service Fédéral Pensions ;
- la FSMA ;
- la Banque Nationale de Belgique (BNB) ;
- l'entreprise de (ré-) assurance avec laquelle la(les) Entreprises d'affiliation et/ou l'OFP ont conclu un contrat (réassurance de la couverture de risques, assurance du fonds de pension, etc.).

Lorsque des données à caractère personnel sont transférées à un sous-traitant, qui sous-traite ces données au nom et pour le compte de l'IRP (le responsable du traitement), l'IRP fait uniquement appel à des sous-traitants qui offrent des garanties suffisantes en ce qui concerne la mise en place de mesures techniques et organisationnelles appropriées par lesquelles le traitement des données est effectué en conformité avec la législation et règlementation en matière de protection des données et par lesquelles les droits des affiliés et des bénéficiaires sont protégés.

L'IRP conclut un contrat écrit avec le sous-traitant qui contient à tout le moins les informations requises par la législation et règlementation en matière de protection des données et qui respecte la politique de sous-traitance de l'IRP. Le contrat prévoit expressément que le sous-traitant peut traiter les données personnelles exclusivement sur la base des instructions écrites de l'IRP et l'IRP prévoit la garantie par le sous-traitant que les personnes qu'il assigne au traitement des données personnelles respecteront la nature confidentielle de ces données. Le contrat prévoit par ailleurs expressément si le sous-traitant est autorisé à travailler avec des sous-traitants et les conditions qui doivent être respectées dans cette hypothèse.

Avant de conclure un contrat avec un sous-traitant, l'IRP vérifie que le sous-traitant puisse fournir des garanties suffisantes qu'il exécutera le traitement des données conformément à la législation et règlementation en matière de protection des données (*due dilligence*). Durant l'exécution de la convention de sous-traitance, l'IRP vérifie le respect de la législation et règlementation en matière de protection des données par le sous-traitant (cf. audits, rapports, ...).

14 Violations de données à caractère personnel

14.1 Mention des violations relatives aux données à caractère personnel

Les utilisateurs autorisés doivent veiller, dans l'exercice de leur fonction dans le cadre de la gestion et de l'exécution des obligations de pension légale (premier pilier), à éviter des incidents (volontaires ou non) qui peuvent porter atteinte à la vie privée des personnes concernées.

En cas de violation de données à caractère personnel, il est d'une importance capitale que des mesures adéquates soient prises le plus rapidement possible pour minimiser le risque de dommage pour les affiliés et bénéficiaires ainsi que pour l'IRP (atteinte à la réputation, sanctions imposées, ...) et l'Entreprise d'affiliation.

L'IRP est tenue d'informer l'Autorité de Protection des Données de toute violation de données à caractère personnel pour laquelle il y a, ou peut y avoir, des conséquences négatives concernant la protection des données à caractère personnel. Cette notification par l'IRP doit intervenir dans les 72 heures suivant la prise de connaissance de la violation de données. Dans certains cas, l'IRP devra également avertir la (les) personne(s) concernée(s) impactée(s) par la violation et cela sans retard déraisonnable.

14.2 Qu'est-ce qu'une violation des données à caractère personnel?

Il est, par exemple, question d'une violation de la sécurité en cas de perte/de vol d'une clé USB, d'un téléphone portable ou d'un ordinateur portable, ou en cas d'intrusion par une personne non autorisée (hacker ou personne bien intentionnée) dans n'importe quel système qui contient des données à caractère personnel, lors de l'envoi d'un courrier ou d'une communication relative à des prestations de pension à une mauvaise adresse. Toutefois, toute violation de la sécurité ne constitue pas une violation relative à des données à caractère personnel. Le tableau ci-dessous montre quand une violation de la sécurité constitue une violation des données qui doit être mentionnée à l'Autorité de Protection des Données et/ou aux affiliés et bénéficiaires concernés.

Dans tous les cas, tous les utilisateurs autorisés, ainsi que toutes les autres personnes qui consultent, utilisent ou gèrent des informations de l'IRP concernant la gestion et l'exécution des obligations de pension légale (premier pilier) sont responsables de signaler immédiatement toute violation de la sécurité et les incidents en lien avec la sécurité des informations au DPO (dont les coordonnées sont reprises ci-après), de sorte qu'une analyse puisse immédiatement être faite, les mesures nécessaires prises et pour savoir si la violation doit être signalée à l'Autorité de Protection des Données et/ou aux affiliés et bénéficiaires concernés et à l'Entreprise d'affiliation.

Les données de contact pour un signalement sont :

DPO : Jean-Francois Henrotte, Boulevard d'Avroy, 280 à 4000 LIEGE, Tél : 04/2220115, e-mail : privacy@ogeofund.be

Lorsque le signalement est réalisé par courriel, il est important que celui-ci soit bien envoyé au DPO de l'IRP et qu'il soit expressément indiqué dans l'objet du courriel qu'il s'agit d'un message avec urgence élevée à propos d'une possible violation en lien avec les données à caractère personnel. Si le DPO de l'IRP ne peut pas être directement contacté par téléphone, il doit en toute hypothèse également être informé par courriel.

Le rapport doit contenir une description complète et détaillée de l'incident, en ce compris l'identité de la personne qui fait le signalement, de quel type d'incident il s'agit, si les données ont trait à des personnes, et combien de personnes sont concernées.

Dans chaque convention avec un sous-traitant, il est précisé que le sous-traitant doit immédiatement signaler toute violation à l'IRP.

14.3 Enquête et analyse des risques

En principe, dans un délai de 24 heures après que l'incident ou la violation a été constaté par l'IRP ou mentionné par un sous-traitant, un utilisateur autorisé, un destinataire, un affilié, un bénéficiaire ou un tiers, une enquête sera entamée par l'IRP et éventuellement par l'entreprise d'affiliation.

L'enquête indiquera quelle est la nature de l'incident, le type de données concernées et si des données à caractère personnel sont concernées (et dans l'affirmative, qui sont les affiliés ou les bénéficiaires concernés et combien de fichiers à caractère personnel sont concernés). L'enquête examinera s'il s'agit d'une violation ou non.

S'il s'agit d'une violation, une analyse des risques sera effectuée pour savoir quelles sont (peuvent être) les conséquences possibles de la violation, et en particulier les impacts (possibles) pour les affiliés et bénéficiaires concernés.

14.4 Gestion et récupération

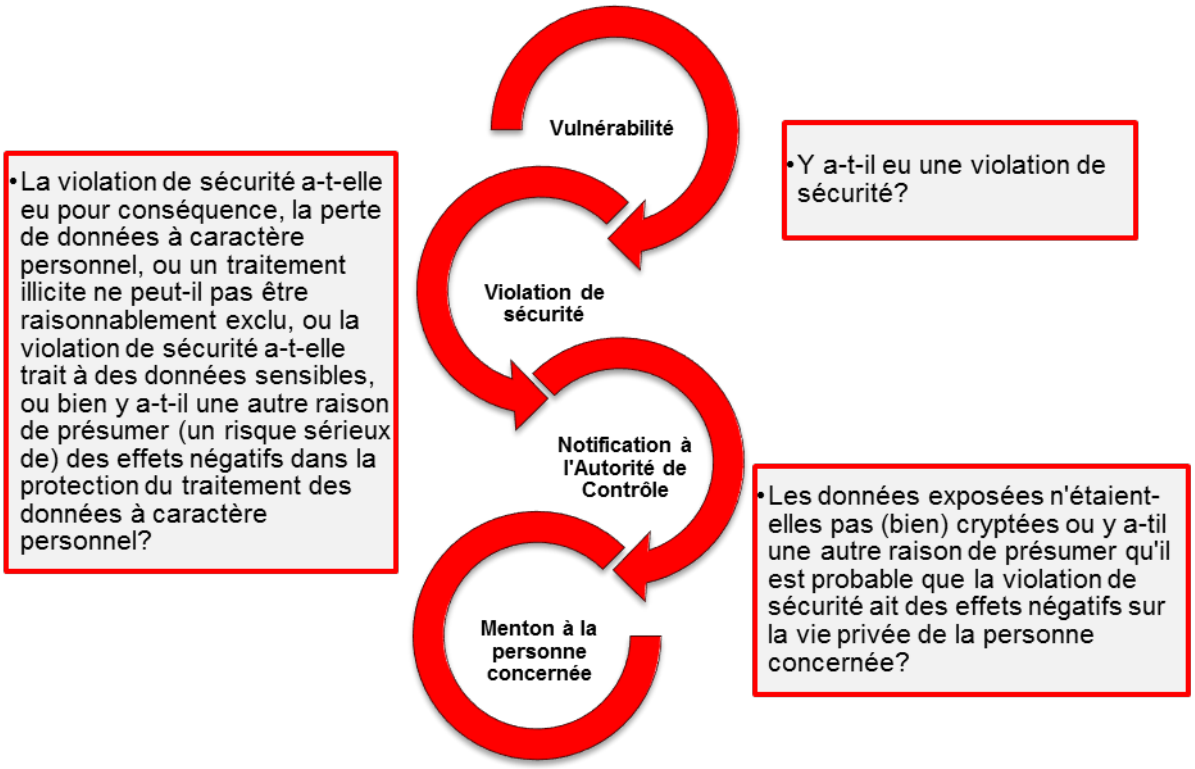
L'IRP veille à ce que des mesures adéquates soient prises pour limiter l'impact de la violation et pour veiller à ce qu'une telle violation ne se reproduise plus à l'avenir. Si nécessaire, un avis d'expert (externe) peut être recueilli pour solutionner rapidement et de manière adaptée la violation et en limiter les conséquences.

14.5 Notification

Pour décider si un certain incident doit être notifié à l'Autorité de Protection des Données, et éventuellement au(x) affiliés et bénéficiaires concerné(s) également, les évaluations suivantes seront faites :

L'IRP insiste encore une fois sur le fait que lorsqu'un utilisateur autorisé, un affilié ou un bénéficiaire ou toute autre personne constatent un incident, il est de la plus haute importance que cet incident soit signalé au DPO de l'IRP, de telle sorte qu'il puisse juger si une (possible) violation a ou non eu lieu et

puisse prendre les mesures et actions nécessaires (parmi lesquelles la notification éventuelle à l'Autorité de Protection des données dans les 72 heures)



14.6 Documentation des violations

L'IRP documente toutes les violations sur la base d'un rapport rédigé par le DPO. Le rapport détaillera la cause principale de l'incident et les facteurs contributifs, la chronologie des événements, les actions en réponse, les recommandations et les leçons apprises en vue d'identifier les domaines qui nécessitent une amélioration. Les changements recommandés aux systèmes, polices et procédures seront documentés et mis en place aussi vite que possible par la suite.

Dans le cadre de sa mission de surveillance du respect de la législation et règlementation en matière de protection des données et de la politique de traitement et de protection des données à caractère personnel dans le cadre de la gestion et de l'exécution des obligations de pension légale (premier pilier) telle que reprise dans le présent Code de conduite, le DPO examinera également les suites données au rapport.

15 Exécution du Code de conduite, sanctions

L'IRP s'assurera que le présent Code de conduite est respecté et dûment appliqué. Toutes les personnes qui ont accès aux données à caractère personnel doivent se conformer au présent Code de conduite.

Les violations à la législation et règlementation en matière de protection des données peuvent conduire à ce que l'IRP soit confrontée à des amendes et/ou des demandes de dommages et intérêts imposées

par l'Autorité de Protection des Données ou la juridiction compétente. Si ces dommages résultent directement d'une violation du présent Code de conduite par un utilisateur autorisé, celui-ci pourra être sanctionné via les actions disciplinaires nécessaires, si applicable comme indiqué dans le règlement de travail, en ce compris, mais pas exclusivement, un licenciement.

16 Communication du Code de conduite

Ce Code de conduite sera communiqué à tous les utilisateurs autorisés actuels et futurs.

L'IRP prévoira une formation périodique sur la politique de traitement et de protection des données à caractère personnel dans le cadre de la gestion et de l'exécution des obligations de pension légale (premier pilier) tel que prévu dans le présent Code de conduite.

L'Entreprise d'affiliation communiquera le présent Code de conduite à tous les travailleurs actuels et nouveaux en le postant sur son intranet ou via un autre moyen de communication collectif.

17 Modifications du Code de conduite

L'IRP se réserve le droit de modifier le présent Code de conduite, selon les besoins, par exemple, en vue de se conformer aux changements dans la loi, les règlements ou les exigences introduites par l'Autorité de Protection des Données. L'IRP et/ou l'entreprise d'affiliation informeront les utilisateurs autorisés ainsi que les affiliés et bénéficiaires de tout changement matériel apporté à ce Code de conduite.

*
* *

Le présent Code de conduite a été établi le 24/05/2018