Degroof Petercam
Trust. Knowledge.

POLITIQUE DE PROTECTION DES DONNÉES

Degroof Petercam

Applicable au 1er janvier 2020

Degroof Petercam

Table des matières

Degroof Petercam

1. Introduction

Le présent document édicte les grands principes applicables pour protéger les données à caractère personnel ainsi que les obligations de l'ensemble des collaborateurs de Degroof Petercam en la matière.

Les collaborateurs, qu'ils soient internes ou externes, s'engagent à respecter les bonnes pratiques édictées dans cette politique qui sont destinées à assurer le respect des règles relatives à la protection des données et à démontrer aisément l'efficacité des mesures prises.

Les rôles et responsabilités relatifs à la protection des données des différents départements sont détaillés dans Data Protection Policy Gouvernance.

2. Contexte général

Le 25 mai 2018, un règlement européen intitulé « Règlement Général sur la Protection des Données » (RGDP) est entré en vigueur dans l'Unions européenne.

L'objectif de ce règlement est d'encadrer l'utilisation et la circulation des données dites à caractère personnel afin de protéger la vie privée des personnes physiques résidant sur le territoire européen en leur offrant une plus grande maîtrise sur les utilisations faites de leurs données personnelles.

Le non-respect du RGDP est fortement sanctionné. Les entreprises qui ne respectent pas la législation encourent :

- des amendes administratives qui peuvent atteindre jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial de l'entreprise ;
- une interdiction temporaire ou définitive de traiter les données ;
- une injonction de se mettre en conformité GDPR ;
- des amendes pénales.

Dans le cadre de ses activités, la Banque Degroof Petercam (ci-après Degroof Petercam) est amenée à traiter de nombreuses données personnelles tant dans le cadre de ses relations avec ses clients, prospects et fournisseurs que pour permettre un fonctionnement optimal de ses ressources humaines.

3. Champ d'application

Le RGDP est un règlement européen et est à ce titre directement applicable dans l'ensemble des Etats Membres de l'Union européenne.

Il est en outre applicable à des traitements de données effectués en dehors de l'Union Européenne mais concernant des personnes physiques qui résident dans l'Union européenne.

Pour cette raison, les dispositions de la présente politique sont également applicables aux traitements effectués par des entités de Degroof Petercam qui ne seraient pas établies dans l'Union Européenne chaque fois que ces traitements concernent des données personnelles de personnes physiques résidant dans l'Union Européenne.

4. Interactions entre les entités de Degroof Petercam

Le présent document contient les principes de base que la direction de Degroof Petercam souhaite voir appliqués dans l'ensemble des entités qui constituent le Groupe.

Dans les cas où, le droit national de certaines entités prévoirait des règles plus strictes, ces règles pourront être inclues dans une politique propre à l'entité. Cependant, elles ne pourront jamais entrer en contradiction avec la présente politique.

Afin de permettre une coordination efficace, toute politique sera présentée pour avis et approbation au Group Data Protection Officer de Degroof Petercam avant d'être soumise aux organes de direction de l'entité concernée.

5. Définitions importantes

- **Donnée à caractère personnel**

  Une donnée à caractère personnel est « toute information se rapportant à une personne physique directement ou indirectement identifiée ou identifiable ».
  Exemples : le nom, le prénom, la date de naissance, le numéro de compte, le numéro de matricule, le numéro de téléphone, l'adresse, une photo, une adresse IP, etc.

- **Données à caractère personnel « sensibles »**

  Exemples de données sensibles : des données relatives à l'origine raciale ou ethnique, aux opinions politiques, aux convictions religieuses ou philosophiques ou à l'appartenance syndicale, ainsi que des données génétiques, des données biométriques, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

- **Traitement de données à caractère personnel**

  Un traitement de donnée à caractère personnel consiste en « toute opération (automatisée ou non) appliquée à des données ou des ensembles de données à caractère personnel. Par opération, on entend notamment : la collecte, l'enregistrement, la consultation, la manipulation, la modification, l'extraction, l'utilisation, le transfert, la diffusion ou toute autre forme de mise à disposition, … ».

  Exemples : collecte d'une carte de visite, consultation sur internet d'informations personnelles, création d'une liste d'invités à un événement, envoi d'un e-mail à un collègue contenant un fichier de données personnelles, collecte d'informations pour compléter le profil investisseur, etc.

- **Responsable du traitement des données** détermine les finalités et les moyens du traitement des données à caractère personnel.

- **Data Protection Officer (DPO)**

  Le DPO doit être associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel conformément aux règles édictes dans la Data Protection Policy Gouvernance.

6. Principes relatifs aux traitements de données à caractère personnel

6.1. REGISTRE DES TRAITEMENTS

Les entités du Groupe tiennent un registre de traitements des données à caractère personnel selon les modalités définies par la loi. La tenue de ce registre est coordonnée par le Data Protection Officer mais le registre est alimenté par les différents départements utilisateurs de données à caractère personnel.

Degroof Petercam est amenée à traiter des données personnelles dans le cadre de ses relations avec :

- ses clients,
- des mandataires,
- des bénéficiaires,
- ses employés,
- des prospects,
- les autorités,
- des fournisseurs,
- d'autres entités.

Le registre doit refléter la réalité des traitements de données personnelles réalisés par chaque entité et permettre d'identifier précisément :

- les parties prenantes (clients, employés, représentant, sous-traitants, co-responsables, etc.) qui interviennent dans le traitement des données ;
- les catégories de données traitées,
- à quoi servent ces données (ce que vous en faites), qui accède aux données et à qui elles sont communiquées,
- combien de temps elles sont conservées,
- comment elles sont sécurisées.

Il est important d'identifier ces éléments car, en fonction des personnes concernées par le(s) traitement(s) de données, les règles en matière de protection des données qui leur sont applicables varieront.

6.2. LICÉITÉ DE TRAITEMENT

Les données à caractère personnel ne peuvent être traitées que pour un usage déterminé, explicite et licite.

Pour ce faire, ce traitement devra :

(i) Se baser sur une des bases de traitement admises ci-après[1] :

[1] Notons que le RGPD prévoit également la possibilité d'un traitement nécessaire à l'exécution d'une mission d'intérêt public. Cette base n'est toutefois par pertinente dans le cadre d'une activité bancaire et donc non retenue comme base valide dans cette politique.

a) Obligation contractuelle **:** La licéité du traitement (ce qui le rend licite) repose sur un contrat dans les situations où le traitement des données personnelles est nécessaire à l'exécution d'un contrat ou l'application de conditions générales de vente (un contrat entre Degroof Petercam et un client) ;

b) Obligation légale (en vertu de la législation UE ou nationale) : Cette licéité s'applique aux cas dans lesquels Degroof Petercam est légalement tenue de procéder à un traitement comme par exemple dans le cadre des obligations en matière de fiscalité ;

c) Intérêt légitime de Degroof Petercam : mais uniquement après avoir vérifié et documenté que les droits fondamentaux et les libertés de la personne dont on traite les données ne sont pas sérieusement affectés.

Si les droits de la personne concernée prévalent sur les intérêts de Degroof Petercam, les données de celle-ci ne peuvent pas être traitées en s'appuyant sur l'intérêt légitime. Afin de déterminer si les intérêts légitimes de traitement de Degroof Petercam prévalent sur ceux de la personne concernée, un « test de balance des intérêts » doit être réalisé dans lequel les circonstances personnelles sont prises en considération.

Exemples :

- *Les responsables du traitement qui font partie d'un groupe d'entreprises ou d'établissements affiliés à un organisme central peuvent avoir un intérêt légitime à transmettre des données à caractère personnel au sein du groupe d'entreprises à des fins administratives internes, y compris le traitement de données à caractère personnel relatives à des clients ou des employés.*

- *Le traitement de données à caractère personnel à des fins de prospection peut être considéré dans certains cas comme étant réalisé pour répondre à un intérêt légitime.*

d) Intérêts vitaux de la personne : Il s'agit des cas où le traitement est nécessaire pour protéger les intérêts vitaux d'une personne par exemple, en cas d'urgence médicale.

e) Consentement de la personne concernée

(ii) se limiter aux finalités pour lesquelles les données ont été collectées

Quelques conseils :

⚠ *Le choix d'une base légale de traitement entraîne des conséquences particulières au point de vue organisationnel. Lorsque que vous souhaitez traiter des données à caractères personnel, veuillez toujours à consulter le département juridique afin de vérifier la légitimité de la base de traitement et déterminer la meilleure option possible.*

⚠ *Pour plus de détails à ce sujet, veuillez également vous référer à la section « Nouveau Traitement de données à caractère personnel ».*

6.3. MINIMISATION DES DONNEES A CARACTERE PERSONNEL ET LIMITATION DE LEUR UTILISATION

Les entités du Groupe veillent à restreindre les informations qu'elles collectent au strict nécessaire. Elles garantissent également au travers de mesures appropriées que l'utilisation des données collectées est restreinte aux finalités pour lesquelles ces données ont été collectées.

6.3.1 Principe de nécessité et minimisation des données

Lorsque Degroof Petercam collecte des données, elle identifie précisément les raisons pour lesquelles elle le fait. L'identification des finalités doit être faite avant de recueillir des données.

Par exemple : l'établissement du profil investisseur du client, l'engagement d'un collaborateur, l'octroi d'un crédit, ou encore l'envoi d'invitations à des évènements, la réalisation d'une campagne marketing, etc.

Degroof Petercam garantit que les données personnelles ne sont traitées que dans la mesure où elles sont adéquates, pertinentes et non excessives par rapport au but poursuivi.

Les collaborateurs évaluent strictement les catégories et la quantité de données personnelles qui sont nécessaires lors d'une collecte de données par rapport à la finalité poursuivie par le traitement.

Quelques exemples pratiques :

⚠ *Ne demandez pas la date de naissance à une personne si la simple collecte de l'âge peut suffire à remplir la finalité poursuivie.*

⚠ *Il n'y a pas non plus de raison de demander à un collaborateur lors de son engagement quels sont ses hobbys ou de demander à un prospect son appartenance religieuse pour l'inscrire à un évènement.*

6.3.2 Limite à l'utilisation des données

Les données doivent en principe être utilisées dans la limite des finalités prévues au moment de la collecte de ses données.

Lorsque Degroof Petercam a l'intention d'utiliser les données à caractère personnel pour une autre finalité que celle pour laquelle les données à caractère personnel ont été obtenues, elle s'engage à vérifier auprès du département juridique si cette nouvelle finalité est compatible avec celle pour laquelle les données ont été initialement collectées.

Par exemple :

- *Le fait qu'une donnée soit publiquement disponible ne signifie pas qu'elle puisse être librement utilisée à d'autres fins. Une donnée peut avoir été collectée et publiée pour respecter des obligations légales comme la publication de comptes annuels (BCE, …). Dans ce cas, elle ne peut être utilisée et publiée que pour la finalité pour laquelle elle a été collectée et ne peut être réutilisée pour du marketing par exemple.*
- *Si les données ont été récoltées sur la base du consentement du client à des fins d'e-marketing pour Degroof Petercam, nous ne sommes pas autorisés à utiliser ces données pour faire du marketing pour des tiers, la finalité n'ayant pas été annoncée.*

6.4. COLLECTE DE DONNÉES

La collecte de données à caractère personnel par une entité du Groupe auprès de tiers internes ou externes au Groupe n'est autorisée que dans le cas où celle-ci répond à une base de traitement licite. A ce titre, les entités du Groupe veillent à ne collecter des informations de tiers que dans la mesure où cette collecte a été formellement approuvée par l'organe compétent, après consultation du Data Protection Officer.

Quelques conseils :

⚠ *Le fait qu'une donnée soit publiquement (ex : internet) disponible ne signifie pas qu'elle peut être librement utilisée.*

⚠ *Tout document organisant une collecte de données personnelles (contrat, formulaire, event form, …) doit faire l'objet d'un contrôle par le département juridique afin de garantir la présence des mentions légales requises.*

⚠ *Toute intention de collecter des données personnelles de manière indirecte doit au préalable faire l'objet d'une demande auprès du Data Protection Officer.*

⚠ *Les collaborateurs veilleront également à respecter les règles en matière de de prospection commerciale définies dans la Politique DPO : Règles à observer en matière de prospection commerciale (not. section 4).*

6.4.1 Distinction entre collecte 'directe et 'indirecte'

Les obligations de Degroof Petercam en termes de transparence varient selon que les données ont été collectées directement auprès de la personne concernée ou indirectement (cf. 6.6. Transparence).

Le RGPD distingue deux types de collecte de données :

- *la collecte de données **directement** auprès de la personne concernée*

Ce type de collecte implique que la personne concernée ait confié des données personnelles directement à Degroof Petercam.

Exemples : il peut s'agir de données obtenues lors de l'onboarding d'un nouveau client ou d'une prise de contact lors d'un évènement via un formulaire ou encore de la situation où une personne souscrite à une newsletter de Degroof Petercam.

Les collaborateurs s'engagent à ce que le traitement de données soit loyal et transparent à l'égard des personnes concernées.

- *la collecte de données **indirecte**, issue d'autres sources*

Dans certains cas, Degroof Petercam obtient des données personnelles sans que la personne concernée ne soit au courant ou même consciente de la collecte de données réalisée.

Par exemple, il peut s'agir de données :

- *reçues d'un partenaire ;*
- *des données publiquement accessibles sur des réseaux ouverts (Moniteur Belge, Banque Nationale de Belgique, Banque-Carrefour, sites internet, blog, réseaux sociaux),*

- *transmises par une institution publique telle que l'administration fiscale, les cours et tribunaux ou le parquet ;*
- *des données qui sont issues de publications dans la presse ;*
- *des données personnelles transmises par des fournisseurs de données professionnels.*

6.4.2 Utilisation de données sensibles

L'utilisation de données sensibles est interdite, sauf dans certaines circonstances exceptionnelles.

Exemples de données sensibles : les données relatives à l'origine raciale ou ethnique, aux opinions politiques, aux convictions religieuses ou philosophiques ou à l'appartenance syndicale, ainsi que des données génétiques, des données biométriques, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

L'interdiction de principe ne s'applique pas si l'une des conditions suivantes est remplie :

- la personne concernée a donné son consentement explicite ;
- le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale, dans la mesure où ce traitement est autorisé par une base légale ;
- le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;
- le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée ;
- le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, ...

⚠ *Toute volonté d'utiliser des données sensibles doit être soumise pour validation au département Legal.*

6.5. TRANSPARENCE VIS-A-VIS DES PERSONNES CONCERNEES

Degroof Petercam doit toujours veiller à ce que les informations relatives à la protection des données soient fournies en temps utiles et accessibles par le client, le lead ou le prospect.

En cas de **collecte directe** auprès de la personne concernée, Degroof Petercam fournira, lors du premier contact avec les personnes concernées, une série d'informations sur les traitements qui seront réalisés sur leurs données (les finalités du traitement, les coordonnées de Degroof Petercam et du DPO, la durée de conservation, les modalités pratiques d'exercice de leurs droits, …).

En cas de **collecte indirecte** des données, Degroof Petercam fournira les informations lors de la première communication avec la personne, et à tout le moins dans un délai ne pouvant excéder 30 jours après avoir obtenu les données personnelles lorsqu'elles sont collectées indirectement. Dans ce cas de figure, Degroof Petercam fournira à la personne concernée des informations additionnelles, telle que la source d'où proviennent les données afin de garantir un traitement équitable et transparent.

⚠ *Veuillez ne pas charger de données dans les systèmes qui ne seront pas utilisées dans les 30 jours.*

Cette communication se fera d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples en utilisant l'un de ces canaux :

- papier ;
- voie électronique ;
- oralement : uniquement lorsque la personne concernée en fait la demande et à condition que l'identité de la personne soit démontrée par d'autres moyens.

Doivent à minima figurer :

- Au bas des sites internet → la Charte vie privée et la Charte Cookies ;
- Sur les communications commerciales papier (pub, invitations, …) → l'identification du responsable de traitement, la Charte vie Privée et la possibilité de s'opposer au traitement
- Sur les communications commerciales par e-mails → l'identification du responsable de traitement, la Charte vie Privée, la possibilité de s'opposer au traitement et les préférences de contact ;
- Lors de chaque collecte de données à caractère personnel → l'identification du responsable de traitement, les raisons de la collecte et la Charte vie Privée.

⚠ *Toute communication commerciale doit être soumise pour validation au département Marketing avant d'être envoyée ou publiée.*

6.6. MESURES DE SÉCURITÉ

Les entités du Groupe garantissent la confidentialité, l'intégrité et la disponibilité des données à caractère personnel au travers de mesures de protection et de contrôles adéquats au regard des risques encourus par la personne concernée.

En tant que Groupe actif dans la prestation de services financiers, Degroof Petercam se doit de garantir un niveau de sécurité élevé pour les données à caractère personnel qu'il traite.

Afin de garantir le niveau de sécurité approprié et de prévenir tout traitement effectué en violation du RGPD, les collaborateurs évaluent les risques inhérents au traitement et mettent en œuvre des mesures pour les atténuer. Ces mesures doivent assurer un niveau de sécurité approprié, y compris en matière de confidentialité, compte tenu de l'état des connaissances et des coûts de mise en œuvre par rapport aux risques et à la nature des données à caractère personnel à protéger.

Dans le cadre de l'évaluation des risques pour la sécurité des données, il convient de prendre en compte les risques que présente le traitement de données, tels que la destruction, la perte ou 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, de manière accidentelle ou illicite, qui sont susceptibles d'entraîner des dommages physiques, matériels ou un préjudice moral.

Ces mesures doivent être élaborées en accord avec les politiques de sécurité de l'information du Groupe.

Ces mesures de sécurité doivent également être imposées aux sous-traitants auxquels Degroof Petercam ferait appel (cf. 6.8 Transfert de données et sous-traitance).

Par exemple : Ces mesures pourraient consister, entre autres, à réduire à un minimum le traitement des données à caractère personnel, à en limiter l'accès, à anonymiser ou pseudonymiser les données à caractère personnel dès que possible, à garantir la transparence en ce qui concerne les fonctions et le traitement des données à caractère personnel, etc.

6.7. TRANSFERTS DE DONNEES ET SOUS-TRAITANCE

6.7.1 Mesures et principes généraux

Les entités du Groupe qui souhaitent faire appel à des sous-traitants veillent à sélectionner ceux-ci avec toute la vigilance requise et s'assurent de la conformité de ces sous-traitants au regard du RGPD et des principes établis au niveau de la présente politique et des autres politiques applicables du Groupe (Outsourcing Policy, Information Security Policy, etc.).

Les collaborateurs de Degroof Petercam doivent identifier et documenter les flux de données à caractère personnel entre les différentes parties et pays impliqués lors :

- de l'élaboration et de la conception de nouveaux produits ou services ;
- de la sélection de nouveaux fournisseurs ou partenaires ;
- de l'utilisation d'applications, de services et de produits qui impliquent le traitement de données à caractère personnel.

6.7.2 Sous-traitance

Lorsqu'elle conclut un contrat avec un prestataire, Degroof Petercam doit déterminer la qualité dans laquelle elle agit d'un point de vue protection des données à caractère personnel et prévoir contractuellement les obligations des parties y relatives.

Le RGDP opère une qualification entre les parties en fonction de certains critères.

Le **responsable du traitement** des données détermine les finalités et les moyens du traitement des données à caractère personnel. Il s'agit d'une notion fonctionnelle, visant à attribuer les responsabilités aux personnes qui exercent une influence de fait, et elle s'appuie donc sur une analyse factuelle plutôt que formelle. Ainsi, si Degroof Petercam décide « pourquoi » et « comment » les données à caractère personnel devraient être traitées, elle est le responsable du traitement.

Degroof Petercam pourrait, dans certains cas, être un **responsable conjoint du traitement** si elle s'associe à une ou plusieurs organisations pour déterminer conjointement « pourquoi » et « comment » les données à caractère personnel devraient être traitées. Les responsables conjoints du traitement doivent conclure un accord déterminant leurs responsabilités respectives pour se conformer aux règles du RGPD. Les principaux aspects de cet accord doivent être communiqués aux personnes dont les données sont traitées.

Le **sous-traitant** quant à lui traite les données à caractère personnel uniquement pour le compte du responsable du traitement. Une activité typique des sous-traitants est de proposer des solutions informatiques. Le sous-traitant des données est généralement un tiers extérieur à l'entreprise. Toutefois, dans le cas des groupes d'entreprises, une entité peut être un responsable du traitement des données, ou un sous-traitant des données, voire les deux.

Le sous-traitant des données ne peut recruter un autre sous-traitant ou nommer un sous-traitant conjoint pour effectuer une partie de sa mission que lorsqu'il a reçu une autorisation écrite préalable du responsable du traitement des données.

⚠ *Les devoirs du sous-traitant envers le responsable du traitement doivent être précisés dans un contrat ou dans un autre acte juridique. Les collaborateurs*

doivent consulter le département juridique afin qu'il les assiste dans la rédaction de ce contrat.

6.7.3 Transferts de données en dehors des de l'Union Européenne

Les transferts de données à caractère personnel en dehors de l'Union Européenne ne peuvent être effectués que dans la mesure où (i) soit les pays vers lesquels sont transférées ces données sont reconnus comme assurant un niveau de protection adéquat, (ii) soit des mesures particulières (notamment l'adjonction de clauses juridiques spécifiques) sont mises en place.

Le GDPR encadre de manière stricte les traitements de données en dehors de l'Union européenne. De tels transferts ne sont autorisés que dans des cas bien précis et doivent faire l'objet d'une analyse. Les entités doivent ensuite monitorer ces transferts et tout souhait de modifier un élément relatif à un transfert de données doit être communiqué sans délai au département juridique.

⚠ *La simple consultation ou le simple accès à des données depuis l'étranger est considéré comme un transfert de données.*

⚠ *Si un flux de données à caractère personnel en dehors de l'Union européenne est envisagé, les collaborateurs doivent consulter le département juridique afin qu'il les assiste pour ce transfert.*

6.8. DROITS DES PERSONNES CONCERNÉES

Les personnes dont les données sont traitées se voient octroyer une série de droits qui leur permettent d'avoir une visibilité sur les traitements réalisés sur leurs données et de garder un contrôle sur celles-ci.

Sous certaines réserves, elles peuvent notamment demander à ce que leurs données soient modifiées, effacées ou transmises. Elles peuvent par ailleurs demander à ce que Degroof Petercam ne traite plus leurs données lorsque le traitement est fondé sur leur consentement ou sur les intérêts légitimes de Degroof Petercam (à moins de prouver que les intérêts de ce dernier sont supérieurs).

Par ailleurs, si des décisions concernant des personnes sont prises sur la base de processus automatisés (en ce compris le profilage), des informations additionnelles doivent être fournies aux personnes concernées et elles doivent avoir le droit de les contester ou de s'y opposer.

⚠ *En pratique, toute question relative aux traitements de données à caractère personnel ou à l'exercice de leurs droits par les personnes concernées doit être transmise immédiatement au Data Protection Officer via l'adresse e-mail dataprivacy@degroofpetercam.com.*

⚠ *La Banque ne dispose que d'un délai de **30 jours** calendriers pour apporter une réponse à la personne concernée.*

6.9. NOUVEAU TRAITEMENT DE DONNEES A CARACTERE PERSONNEL

6.9.1 Mise à jour du registre de traitements

Tout nouveau traitement de données doit être analysé et autorisé préalablement par le département juridique. Il doit ensuite être communiqué sans délais au Data Protection Officer conformément à la Procédure sur la tenue du registre des traitements de données.

Les entités du Groupe sont activement responsables de la mise en conformité des nouveaux traitements de données par rapport à la présente politique, le cas échéant en se basant sur les procédures auxquelles il est fait référence dans la présente politique.

Ils identifient les nouveaux traitements de données à caractère personnel lorsqu'ils envisagent une nouvelle finalité de traitement, négocient un nouveau contrat ou développent un nouveau projet, activité ou processus.

⚠ *Si des données à caractère personnel font l'objet d'un ou plusieurs traitements, les collaborateurs détermine précisément :*

- *de quelles données il s'agit ;*
- *quelles sont les personnes à qui elles appartiennent ;*
- *d'où elles proviennent ;*
- *ainsi que leur qualité.*

Pour chaque nouveau traitement de données à caractère personnel, les entités de Degroof Petercam s'engagent à remplir le registre des traitements de données.

Toute modification apportée aux conditions de mise en œuvre d'un traitement existant inscrit au registre (nouvelle donnée collectée, allongement de la durée de conservation, nouveau destinataire du traitement, etc.) doit également être portée au registre par les collaborateurs.

6.9.2 Procéder à une analyse d'Impact

Chaque traitement de données à caractère personnel doit faire l'objet d'une appréciation des risques mais aussi des mesures mises en place pour faire face aux risques (les garanties, les mesures de sécurité et les mécanismes pour assurer la protection des données à caractère personnel) et pour démontrer que le RGPD a été respecté.

Ce n'est qu'après la prise en considération des mesures de protection visées que l'on peut évaluer le risque résiduel du traitement envisagé.

Si le traitement envisagé est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées, les entités veilleront à réaliser un DPIA selon les modalités spécifiées dans la Procédure : Data Protection Impact Assessment. Le DPIA sera soumis à l'approbation du DPO.

Par exemple : Un risque élevé survient lorsque des mécanismes de traitement automatisé et de profilage sont utilisés pour examiner de manière systématique et considérable les personnes concernées ; un espace public est systématiquement surveillé à grande échelle (par exemple, au moyen de la vidéosurveillance) ; des données sensibles sont traitées à grande échelle (par exemple, des données médicales).

Si les mesures de sécurité envisagées ne permettent pas de supprimer tous les risques élevés relevés, l'Autorité de protection des données doit être consultée avant que le traitement des données envisagé ne débute.

6.10. NOTIFICATION DE FUITES DE DONNEES (DATA BREACH)

> En cas d'incident de sécurité pouvant mettre en péril la confidentialité, l'intégrité ou la disponibilité des données de personnes concernées, les entités du Groupe doivent en informer immédiatement le Data Protection Officer via l'adresse e-mail : dataprivacy@degroofpetercam.com

Un data breach est 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.

En cas de data breach, les entités mettent en place le plus rapidement possible les mesures nécessaires afin d'en limiter l'impact et les effets. Elles informent le DPO afin que celui-ci puisse vérifier l'adéquation des mesures mises en place par l'entité.

Dans ce contexte, le DPO prend en charge l'évaluation des risques pour les personnes concernées et les démarches nécessaires en cas d'éventuelles notification aux régulateurs ou à la personne concernée.

Le DPO du Groupe doit notifier une fuite de données à l'Autorité de protection des données lorsqu'il existe un "risque pour les droits et libertés de la personne concernée".

Par exemple, il peut s'agir d'une perte de confidentialité d'une communication, rendant temporairement des données transactionnelles, des adresses, etc. accessibles à des tiers.

Le DPO a par ailleurs l'obligation de signaler la violation à la personne concernée lorsqu'il y a un risque élevé pour cette dernière.

6.11. CONSERVATION ET SUPPRESSION DES DONNEES

> Degroof Petercam s'engage à ne pas conserver les données qu'elle a collectée sous une forme permettant l'identification des personnes concernées pour une durée supérieure à celle qui est nécessaire pour mener à bien la ou les finalité(s) d'un traitement spécifique.

Pour ce faire, Degroof Petercam adopte une Politique de rétention des données à caractère personnel qui reprend en détail les délais de conservation pour chaque grande catégorie de données et que les collaborateurs s'engagent à respecter.

Dans certains cas, la personne concernée peut obtenir de Degroof Petercam, dans les meilleurs délais, l'effacement de tout ou partie de ses données, par exemple lorsque ces données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ou lors du retrait du consentement donné par la personne concernée sans que les traitements ne puissent encore être justifiés.

Degroof Petercam

7. Liens avec d'autres politiques et procédures

Cette politique a un lien avec les politiques et procédures suivantes.

Réf.	Procédure/Politique
1.	**Politique de gouvernance des données à caractère personnel**
2.	**Politique DPO : Règles à observer en matière de prospection commerciale**
3.	**Politique de rétention des données**
4.	**Data Subject Deletion Request Procedure**
5.	**Information Security Policy**
6.	**Enterprise Data Management Policy V02.3 CDO**

8. Sources légales et réglementaires

N°	Type (loi, règlement, circulaire…)	Source
1.	**Règlement européen**	RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL 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), entré en vigueur le 25 mai 2018
2.	**Directive européenne**	Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)
3.	**Code de droit économique**	Livre VI et XII
4.	**Loi**	30 JUILLET 2018. - Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel
5.	**Arrêté Royal**	4 AVRIL 2003 - Arrêté royal visant à réglementer l'envoi de publicités par courrier électronique