CPVP
Commission de la protection de la vie privée

RGPD

vade-mecum pour les PME

Un guide pour préparer les petites et moyennes entreprises (PME) au Règlement général sur la protection des données

janvier 2018

Objectif du présent document

Le Règlement général sur la protection des données (RGPD) entre en vigueur le 25 mai 2018. La Commission de la protection de la vie privée (CPVP) veut informer et assister les PME dans la mise en œuvre de cette nouvelle règlementation. Dans la brochure, il est parfois question de l'APD, il s'agit de l'Autorité de protection des données qui remplacera la CPVP à partir du 25 mai 2018.

Il n'est toutefois pas possible de rédiger une brochure qui réponde aux besoins spécifiques de chaque PME individuelle. L'impact du RGPD sur le fonctionnement quotidien d'une PME dépend en effet en premier lieu des activités de traitement de cette PME et non du statut de la PME en soi. La diversité des activités de traitement effectuées par les PME est trop grande pour être reprise dans un seul document.

Nous invitons dès lors les fédérations sectorielles à retravailler ce document de base et à l'adapter à la spécificité de leur secteur (sous la forme de modèles, de codes de conduite, de lignes directrices, etc.). La CPVP est convaincue que les fédérations sectorielles sont les mieux placées pour traduire concrètement le RGPD dans le contexte sectoriel et cartographier les risques spécifiques par secteur.

La présente brochure entend donner un aperçu succinct des principaux droits et obligations qui découlent du RGPD et qui sont pertinents pour les PME. Elle n'a pas l'ambition d'aborder de manière exhaustive toute la législation applicable en matière de protection des données. Les exemples cités et les explications relatives au RGPD aident à comprendre le RGPD mais n'ont aucune valeur de précédent juridique. En outre, chaque application du RGPD requiert toujours une analyse concrète, adaptée à chaque situation spécifique.

Sommaire

Lexique

RGPD	Le Règlement général sur la protection des données
CPVP	La Commission de la protection de la vie privée
APD	L'Autorité de protection des données. Le 25 mai 2018, l'APD succédera à la Commission de la protection de la vie privée en tant qu'autorité de contrôle au sens du RGPD.
Le Groupe 29	Le Groupe de travail de l'Article 29 sur la protection des données. Le groupe comprend les contrôleurs nationaux des Etats membres de l'Union européenne, dont la CPVP, et émet des avis sur l'application de la législation européenne en matière de protection de la vie privée. À partir du 25 mai 2018, le Comité européen de la protection des données remplacera le Groupe de travail de l'Article 29 sur la protection des données.
DPO	Le délégué à la protection des données – aussi appelé en anglais Data protection Officer (DPO).
AIPD	L'analyse d'impact relative à la protection des données - aussi appelée en anglais Data Protection Impact Assessment (DPIA).
Violation de données à caractère personnel	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- aussi appelée en anglais Data Breach.

Introduction

Le RGPD instaure une règlementation harmonisée en matière de protection des données qui sera directement applicable au sein de toute l'Union européenne. En principe, le RGPD s'applique de la même manière dans le secteur public et dans le secteur privé et cette législation vaut aussi bien pour les grandes entreprises que pour les PME. Attention : sur plusieurs points, les États membres de l'Union européenne peuvent ou doivent adopter des dispositions nationales qui viendront compléter le RGPD. Les règles de protection des données s'appliquent dans des domaines variés, eux-mêmes réglementés. Dès lors, en plus du RGPD, tenez toujours compte de la législation nationale spécifique. L'on ne vise pas exclusivement par là le droit à la protection des données mais également d'autres domaines du droit, tels que le droit du travail.

Le nouveau RGPD se fonde sur la législation actuelle. Les concepts et principes fondamentaux à la base du traitement de données à caractère personnel sont globalement maintenus. Si votre PME répond à la loi belge sur la protection de la vie privée, vous êtes déjà en bonne voie pour également respecter le RGPD. Le RGPD y ajoute plusieurs nouveaux éléments pour adapter la législation aux développements technologiques rapides des vingt dernières années.

Les nouvelles obligations créées par le RGPD peuvent se résumer en trois lignes de force : l'approche basée sur les risques, la responsabilité et la transparence :

- ***L'approche basée sur les risques*** signifie que les obligations qui découlent du RGPD varient en fonction du risque lié à l'activité de traitement. Le RGPD crée donc une marge pour parvenir à une solution sur mesure pour chaque PME.
- ***La responsabilité*** implique qu'un responsable du traitement doit pouvoir démontrer le respect du RGPD. Dès lors, la documentation des choix est importante de manière à ce qu'une PME puisse justifier les raisons pour lesquelles elle a ou non instauré une mesure déterminée.
- ***La transparence*** est cruciale, tant en interne qu'en externe. En interne, vous devez avoir une idée claire de tous les traitements de données à caractère personnel sous la responsabilité de votre PME et vous devez sensibiliser le personnel à ce sujet. En externe, vous devez informer plus clairement les personnes dont vous traitez les données quant à leurs droits, à la manière dont elles peuvent exercer ces droits et aux tenants et aboutissants de l'activité de traitement.

La présente brochure a tout d'abord été rédigée du point de vue de la PME en tant que responsable du traitement. Les obligations qui s'appliquent aux responsables du traitement et aux sous-traitants ne sont pas identiques. C'est pourquoi la rubrique reprise sous le titre V Checklist pour le sous-traitant explique brièvement quelles sont les obligations applicables aux sous-traitants. Attention : votre PME peut parfois être aussi bien un responsable du traitement qu›un sous-traitant. Pour de plus amples informations sur les notions de sous-traitant et de responsable du traitement, voir le titre I Notions de base.

I. Notions de base – est-ce que moi aussi je traite des données à caractère personnel ?

Le RGPD s'applique si votre PME *traite des données à caractère personnel*.

- **Les données à caractère personnel** sont toute donnée se rapportant à une personne physique identifiée ou identifiable (article 4.1 du RGPD). Lorsque le couplage d'éléments d'information (âge, sexe, code postal, etc.) peut conduire à l'identification unique d'une personne ('singling out'), chaque élément constitue également une donnée à caractère personnel. Des données à caractère personnel pseudonymisées[1] pour lesquelles il existe une clé permettant d'obtenir à nouveau les données à caractère personnel initiales sont également des données à caractère personnel. Des données anonymes[2] ne constituent pas des données à caractère personnel. Le RGPD ne s'applique par contre pas aux données relatives à des personnes décédées ou de personnes morales.

o **EXEMPLE:**

  - Sont des données à caractère personnel :
  - les nom, prénom et coordonnées de clients, de membres du personnel ou de fournisseurs (personnes physiques) ;
  - l'historique des achats, les factures impayées, les informations de paiement (pour autant qu'elles concernent des personnes physiques) ;
  - les évaluations du personnel et attestations médicales ;
  - les informations relatives aux pages Internet visitées par une adresse IP ;
  - les données de localisation (par ex. localisation via une application d'un smartphone) ;
  - une liste des matricules des personnes qui travaillent à mi-temps ;
  - des images vidéo et plaques d'immatriculation.

Ne sont pas des données à caractère personnel :

  - l'adresse e-mail générale ou le numéro de téléphone général de la PME- par ex. PME@email.be;
  - le numéro d'entreprise (sauf dans le cas d'une entreprise unipersonnelle).

- **Les données sensibles** sont les données à caractère personnel qui méritent un niveau de protection plus élevé car leur traitement peut entraîner des risques significatifs. Le traitement de données sensibles est en principe interdit, à moins que vous ne satisfaisiez à l'un des motifs d'exception de l'article 9 ou de l'article 10 du RGPD. Des données à caractère personnel ordinaires vous permettant de déduire des informations sensibles constituent également des données sensibles. Il s'agit de :

  - catégories particulières de données à caractère personnel (article 9 du RGPD). Font partie de ce groupe les données relatives à la santé, les données génétiques et les données biométriques en vue de l'identification unique d'une personne. Les données à caractère personnel qui révèlent l'origine raciale ou ethnique, la vie sexuelle ou l'orientation sexuelle, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale font aussi partie de cette catégorie particulière ;
  - données judiciaires relatives aux condamnations pénales et aux infractions (article 10 du RGPD).

o **EXEMPLE:**

  - une application sportive qui mesure la vitesse, la distance, la fréquence cardiaque et la quantité de calories brûlées peut dévoiler des informations sur l'état de santé d'une personne ;
  - un extrait du casier judiciaire.

- **La notion de traitement** est très large et comprend toute opération effectuée ou non à l'aide de procédés automatisés et appliquée à des données à caractère personnel (article 4.2 du RGPD). Des exemples de traitement sont 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.

1 Le RGPD utilise le terme pseudonymisation pour faire référence à des données codées qui ne peuvent plus être attribuées à une personne physique précise sans informations supplémentaires servant de clé.

2 Contrairement à ce qui vaut pour les données à caractère personnel pseudonymisées, pour les données anonymes, il n'existe plus aucune clé permettant d'identifier la personne physique. Un exemple : les données statistiques agrégées.

⚠ Bien que le RGPD vise principalement les traitements automatisés de données à caractère personnel (comme l'enregistrement sur un support numérique), vous ne pouvez pas contourner la loi en conservant toutes les données à caractère personnel sur des supports papier. La conservation sur papier de fichiers systématiquement organisés constitue également un traitement au sens du RGPD.

- **EXEMPLE :**
  - la collecte de données clients via une page Internet afin de procéder à des achats en ligne ;
  - la tenue de fiches papier systématiquement organisées avec les données clients ;
  - la conservation, la consultation et la gestion numériques de données RH de votre personnel.

- Il est également important de déterminer les **acteurs** auxquels s'applique le RGPD. L'instance qui détermine les finalités et les moyens du traitement est le **"responsable du traitement"** (article 4.7 du RGPD). L'entreprise qui traite des données à caractère personnel pour le compte d'un responsable du traitement est ce qu'on appelle le **"sous-traitant"** (article 4.8 du RGPD). Les personnes identifiables ou identifiées dont des données à caractère personnel sont traitées, telles que des clients ou des membres du personnel, sont également désignées dans le présent document par les termes **"personnes concernées"** (article 4.1 du RGPD). Les personnes décédées ou les personnes morales ne sont pas considérées comme des "personnes concernées".

- **EXEMPLE:**
  - une PME est le responsable du traitement des données de ses clients et de son personnel ;
  - un secrétariat social qui traite des données RH pour d'autres entreprises est souvent un soustraitant ;
  - un fournisseur de cloud auquel une PME a recours pour stocker des données est souvent un sous-traitant.

Pour de plus amples informations

- Article 4 du RGPD- Définitions
- Avis 4/2007 du Groupe 29 sur la notion de donnée à caractère personnel- WP 136

II. Obligations - de quoi dois-je tenir compte ?

Le RGPD s'applique à tout traitement de données à caractère personnel et ne fait en principe pas d'exceptions pour les PME. Une PME doit donc toujours respecter les principes de base qui constituent le fondement de chaque traitement licite de données à caractère personnel (Titre II.1 Principes de base).

Cela ne signifie pas que le RGPD place la barre à la même hauteur pour chaque PME. Une PME ne doit prendre certaines mesures que si un traitement est lié à des risques particuliers, mesures telles que par exemple la désignation d'un délégué à la protection des données (DPO) ou la réalisation d'une analyse d'impact relative à la protection des données (AIPD), (Titre II.2 Mesures de protection adaptées aux risques.)

En outre, ce chapitre attire l'attention sur les obligations du sous-traitant et du responsable du traitement lorsque ce dernier a recours à un prestataire de services externe- un sous-traitant donc- (outsourcing). La sous-traitance de données dans le cloud ou dans un centre de données mais aussi la sous-traitance d'une administration du personnel en sont des exemples courants. (Titre II.3 Prestataires de services externes).

Enfin, les PME doivent respecter des garanties complémentaires lors de la transmission de données à caractère personnel en dehors de l'Union européenne (Titre II.4 Où vont vos données ?).

1 Principes de base

1.1 Base juridique

Chaque traitement de données à caractère personnel doit reposer sur une des bases juridiques énumérées à l'article 6 du RGPD. Le RGPD distingue six bases juridiques différentes : le consentement, le contrat, le respect d'une obligation légale, la sauvegarde d'un intérêt vital, l'exécution d'une mission d'intérêt public et l'intérêt légitime poursuivi par le responsable du traitement ou par un tiers.

Une PME invoquera principalement **le consentement, le contrat, le respect d'une obligation légale** et **l'intérêt légitime**. Toutes ces bases juridiques sont équivalentes et il appartient à la PME de choisir la base juridique qui correspond le mieux à ses activités de traitement.

⚠ Attention : si vous traitez des données sensibles, outre une de ces bases juridiques, vous devez également satisfaire à un des motifs d'exception prévus à l'article 9.2 ou à l'article 10 du RGPD !

TO DO

Documentez la base juridique pour chaque traitement.

Pour de plus amples informations

- ❖ Article 6 du RGPD- Licéité du traitement
- ❖ Article 9 du RGPD- Traitement de catégories particulières de données à caractère personnel
- ❖ Article 10 du RGPD – Traitement de données à caractère personnel relatives à des condamnations pénales

1.1.1. Le consentement

Une PME peut traiter des données à caractère personnel si la personne concernée y consent. Attention toutefois : le consentement n'est pas une solution miracle qui équivaut à une acceptation des conditions générales ! De plus, la personne concernée peut toujours et sans la moindre motivation retirer son consentement.

Selon la définition à l'article 4.11 du RGPD, chaque consentement doit :

- être **libre**. Les personnes concernées doivent avoir un *véritable* choix, sans être mises sous pression avec le risque de conséquences négatives si elles ne donnent pas leur consentement. Un consentement qui est indissociablement lié à l'acceptation de conditions générales n'est pas valable.
    - **EXEMPLE** :
    - dans la relation entre un employeur et un travailleur, le consentement sera rarement libre en raison du lien de subordination qui existe entre eux ;
    - une PME développe une application qui aide les utilisateurs à apprendre les langues. Lors de l'installation, afin de pouvoir utiliser l'application, les utilisateurs doivent lui donner l'autorisation d'activer leur localisation GPS. La PME utilise ces informations à des fins commerciales. La géolocalisation de l'utilisateur n'est toutefois pas nécessaire pour le fonctionnement de l'application. Étant donné que l'utilisateur ne peut pas utiliser l'application sans consentir à la géolocalisation, le consentement n'est pas libre.
- être **spécifique**. Cela signifie que la personne concernée doit avoir, pour chaque finalité distincte, le choix de consentir ou non.
    - **EXEMPLE** : une PME demande un seul consentement afin de tenir les clients au courant de nouvelles offres et de partager leurs données clients avec des partenaires commerciaux. Ce consentement n'est pas spécifique car on ne peut pas consentir séparément à une des deux finalités.
- être **informé**. Cela signifie que la PME doit expliquer au préalable à la personne concernée dans un langage compréhensible qui utilisera quelles données à caractère personnel et pour quelles finalités. Une PME doit également toujours signaler à la personne concernée la possibilité de retirer le consentement. Il faut clairement distinguer toutes ces informations de toutes les autres informations ou des dispositions contractuelles.
    - **EXEMPLE** : un paragraphe dans les conditions générales contenant des informations sur le traitement de données à caractère personnel ne conduit pas à un consentement informé.
- reposer sur une action **positive**.
    - **EXEMPLE** : **:** le consentement ne peut pas être déduit d'une case pré-cochée dans un formulaire (opt-out).

En outre, un consentement valable doit également satisfaire un certain nombre d'exigences supplémentaires. Ainsi, le consentement doit aussi :

- être **démontrable**. Vous devez toujours garder une preuve de l'obtention du consentement.
- **pouvoir être retiré tout aussi facilement qu'il a été donné.**

- **EXEMPLE :** lors d'un achat en ligne, un client consent à recevoir de la publicité de la PME en cochant une case. Pour retirer ce consentement, le client doit téléphoner à la PME. Étant donné qu'un appel nécessite plus de démarches qu'un simple clic de souris, le consentement n'est pas valable.

Le consentement qui a été donné en vertu de la législation belge relative à la vie privée ne reste valable que dans la mesure où celui-ci est conforme au RGPD !

- **EXEMPLE** : vous avez recueilli le consentement pour traiter des données à caractère personnel via une case pré-cochée. En vertu du RGPD, cela n'est plus possible ! Vous devez donc demander un nouveau consentement à la personne concernée avant le 25 mai afin de poursuivre le traitement.

⚠ Attention : vous pouvez également traiter des données sensibles sur la base du consentement. Dans ce cas, le consentement doit aussi être "explicite". La barre pour un consentement explicite se situe plus haut que pour un consentement ordinaire et exige une déclaration expresse de consentement. Cela peut par exemple se faire au moyen :

- d'une déclaration numérique ou écrite signée (électroniquement) de la personne concernée ;
- d'une double confirmation par mail et/ou SMS (double opt-in).

Pour de plus amples informations

- Article 7 du RGPD- Conditions applicables au consentement
- Article 4.11- Définitions
- Lignes directrices du Groupe 29 sur le consentement en vertu du Règlement 2016/679- WP259

1.1.2. Le contrat

Lors de la conclusion d'un contrat, une PME peut traiter les données à caractère personnel d'un client, d'un membre du personnel ou d'un fournisseur qui sont nécessaires à l'exécution de ce contrat. Cette base juridique couvre également les mesures précontractuelles à condition qu'elles soient exécutées à la demande de la personne concernée. L'initiative doit donc venir de la personne concernée. Cette nécessité ne peut pas être interprétée au sens large et se limite aux données à caractère personnel sans lesquelles le contrat ne *peut* pas être exécuté.

- **EXEMPLE:**

  - une PME doit, en tant qu'employeur, traiter des données à caractère personnel de ses travailleurs pour payer le salaire. Ce traitement est nécessaire pour exécuter le contrat de travail ;
  - un client demande à une PME une offre. Afin d'envoyer cette offre et en attendant l'acceptation de celle-ci, la PME peut, en s'appuyant sur cette base juridique, temporairement conserver les coordonnées du futur client ;
  - dans le cadre de la vente de biens en ligne, une PME peut traiter des données à caractère personnel telles que le nom, l'adresse et les données de carte de crédit afin de permettre le paiement et la livraison ;
  - dans le cadre de la vente de biens en ligne, cette base juridique ne suffit pas pour établir un profil d'utilisateur s'appuyant sur les habitudes d'achat et de clic de l'utilisateur. Bien que ces informations puissent peut-être fournir à la PME un avantage économique, ces données à caractère personnel ne sont pas nécessaires à l'exécution du contrat d'achat proprement dit.

⚠ Attention : si vous traitez des données sensibles, votre traitement ne peut pas reposer sur cette base juridique !

1.1.3. L'obligation légale

Une PME peut traiter des données à caractère personnel si la loi l'impose. Pour une PME, cette base juridique est par exemple importante pour transmettre des données à caractère personnel de membres du personnel au fisc ou aux institutions de la sécurité sociale.

- **EXEMPLE :**l'arrêté royal du 5 novembre 2002 instaurant une déclaration immédiate de l'emploi (déclaration DIMONA) prescrit que l'employeur communique à l'Office national de sécurité sociale (ONSS) des données à caractère personnel d'un travailleur. L'autorité utilise ces données pour attribuer certains droits sociaux au travailleur.

⚠ Attention : si vous traitez des données sensibles, l'obligation légale en question doit faire partie d'une des catégories de l'article 9.2 du RGPD !

1.1.4. L'intérêt légitime du responsable du traitement

Une PME peut traiter des données à caractère personnel si cela est nécessaire aux fins de l'intérêt légitime poursuivi par le responsable du traitement ou par un tiers, sauf lorsque les intérêts ou les libertés et droits fondamentaux de la personne concernée prévalent. Cela signifie que la PME doit d'abord poursuivre un intérêt légitime pour ensuite réaliser une mise en balance avec les intérêts de la personne concernée. Cette base juridique est donc dynamique et requiert pour chaque traitement une légitimation spéciale et documentée qui prend en considération les besoins de la PME par rapport à l'impact sur la personne concernée.

- **EXEMPLE :**
  - le marketing direct (ou "prospection" au sens du RGPD) constitue une méthode courante pour faire de la prospection. Si le marketing direct n'est pas trop fréquent et agressif, la PME peut utiliser des coordonnées dans le cadre d'une relation de clientèle existante à des fins de marketing direct pour promouvoir ses propres services ou produits. Attention : l'article 13 de la Directive e-Privacy (Directive 2002/58/CE)[3] impose plusieurs conditions supplémentaires. Lors de la collecte des coordonnées, la PME doit signaler explicitement au client son droit de s'opposer au marketing direct. La PME doit faciliter l'exercice de ce droit (par ex. via une possibilité d' "opt-out" visible claire lors de la collecte des données et lors de chaque communication de marketing direct) ;
  - en vertu de cette base légale, les PME peuvent traiter des données à caractère personnel qui sont nécessaires pour détecter une fraude à la facturation et pour en informer leurs clients.

⚠ Attention : si vous traitez des données sensibles, votre traitement ne peut pas reposer sur cette base juridique !

1.2. Finalité

Le principe de finalité est un fondement crucial du RGPD. Selon l'article 5.1.b) du RGPD, vous ne pouvez traiter des données à caractère personnel que pour des finalités qui ont été définies explicitement au préalable. En principe - mais il existe des exceptions -, il est interdit de traiter ultérieurement les données obtenues pour une autre finalité qui n'était pas prévue initialement. Il s'agit du principe de base.

Trois possibilités se présentent si vous souhaitez quand même traiter des données à caractère personnel pour une finalité qui diverge de celle pour laquelle vous avez initialement traité ces données :

- **Consentement distinct** : vous demandez le consentement de la personne concernée afin de traiter les données à caractère personnel pour cette nouvelle finalité. Ce consentement constitue la base juridique du traitement pour cette nouvelle finalité ;
  - **EXEMPLE** : une PME développe un profil de client sur la base des habitudes d'achat et de clic sur son site Internet. Le client a ainsi consenti à optimaliser son expérience d'utilisateur et à rester informé d'offres spéciales qui pourraient l'intéresser. Si la PME souhaite revendre ultérieurement ces profils à un courtier en données à des fins publicitaires, elle doit pour cela demander distinctement le consentement du client ;
- **Obligation légale** : le traitement ultérieur de données à caractère personnel découle d'une obligation légale. L'obligation légale constitue en l'occurrence la base juridique du traitement ultérieur.
- **Compatibilité** : le responsable du traitement doit évaluer si la nouvelle finalité est ***compatible*** avec les finalités pour lesquelles les données ont été obtenues initialement. Si tel est le cas, le traitement repose sur la base juridique qui vous a permis d'obtenir et de traiter initialement les données.
  - **EXEMPLE** :
    - une PME installe une caméra de surveillance à l›entrée de son magasin. La caméra filme également fortuitement la caissière qui accueille les clients et répond au téléphone. La PME ne peut en principe utiliser ces images vidéo qu'en cas d'incident de sécurité (par ex. un braquage) et pas pour évaluer les prestations de travail de la caissière.

Le RGPD énumère quelques critères qui peuvent aider à vérifier si la nouvelle finalité est compatible ou non avec la finalité initiale. Ces critères vérifient si ce traitement ultérieur était raisonnablement prévisible pour la personne concernée. La PME doit donc tenir compte :

3 Au moment de rédiger la présente brochure, la Directive e-Privacy est en cours de révision. La Commission européenne a pris l'initiative de convertir la Directive e-Privacy en un Règlement e-Privacy. Cette règle peut donc changer à l'avenir.

- du lien entre les finalités initiales et les nouvelles finalités ;
- du contexte dans lequel les données à caractère personnel ont été collectées, eu égard en particulier à la relation entre les personnes concernées et le responsable du traitement ;
- de la sensibilité et de la nature des données à caractère personnel, surtout si le traitement concerne des catégories particulières de données à caractère personnel ;
- des conséquences possibles du traitement ultérieur pour les personnes concernées ;
- de l'existence de garanties appropriées, dont le cryptage ou le codage.

o **EXEMPLE :** une PME fournit à domicile des repas préparés avec des ingrédients locaux. La PME veut utiliser les coordonnées et l'historique des achats afin d'appliquer des offres spéciales ou une réduction sur ses propres repas. Cette utilisation est compatible avec la finalité initiale, étant donné qu'il existe un lien étroit entre la prestation de services et les offres spéciales, que les données ne sont pas sensibles et que les conséquences pour le client sont positives. Attention : cette analyse peut prendre une autre tournure si la PME utilise un profilage très poussé ou lorsque cela conduit à une différenciation de prix[4].

TO DO

Vérifiez que chaque traitement de données à caractère personnel a une finalité déterminée, explicite et légitime et que si ces données sont réutilisées pour une finalité autre que la finalité initiale, la nouvelle utilisation des données est compatible avec la première utilisation.

Pour de plus amples informations

- ❖ Article 5.1.b) du RGPD – Principes relatifs au traitement des données à caractère personnel
- ❖ Article 6.4 du RGPD- Licéité du traitement
- ❖ Avis 03/2013 du Groupe 29 sur la limitation de la finalité – WP 203

1.3. Exactitude et qualité des données

Les données à caractère personnel doivent être exactes et actuelles. Dès qu'une PME prend conscience du caractère erroné ou dépassé des données à caractère personnel, elle doit les actualiser, les rectifier ou les effacer. Bien qu'une PME n'assume pas la responsabilité finale si un client ou une autre personne concernée communique des informations erronées, elle doit toutefois fournir des efforts proactifs pour détecter et rectifier des erreurs évidentes. La personne concernée dispose d'ailleurs également d'un droit de rectification de ses données à caractère personnel (voir à cet effet le titre III. Droits de la personne concernée).

Ce principe a également des conséquences pour le délai de conservation de données à caractère personnel. Si vous conservez des données trop longtemps, celles-ci ne sont plus exactes. Définissez donc une politique conçue de manière à ce que les anciennes données à caractère personnel soient systématiquement effacées ou actualisées.

o **EXEMPLE:**

– quand un client ou un membre du personnel communique un changement, la PME doit appliquer ce changement le plus rapidement possible. Cette modification peut concerner le nom, l'adresse, le domicile, l'adresse e-mail, le numéro de téléphone, le nombre d'enfants à charge, la plaque d'immatriculation, etc.

TO DO

Contrôlez activement vos données clients afin de détecter des adresses e-mail inexactes et de vérifier la correspondance entre le code postal et le nom de la rue. Contactez votre client si vous soupçonnez que les données sont erronées et adaptez-les si nécessaire.

Pour de plus amples informations

- ❖ Article 5.1.d) du RGPD – Principes relatifs au traitement des données à caractère personnel
- ❖ Article 16 du RGPD- Droit de rectification

4 Comme précisé plus haut, la PME doit informer explicitement le client que celui-ci a le droit de s'opposer au marketing direct et elle doit faciliter l'exercice de ce droit pour le client.

1.4. Traitement de données minimal

La collecte et le traitement de données à caractère personnel doivent se limiter à ce qui est strictement nécessaire pour réaliser les finalités envisagées. Les données réclamées doivent être pertinentes. Cela signifie qu'une PME doit pouvoir démontrer pour chaque donnée à caractère personnel pour quelles raisons ces informations sont nécessaires pour atteindre la finalité. Si la PME ne peut pas le démontrer, les données à caractère personnel sont excessives et doivent être effacées.

o **EXEMPLE:**

- une PME utilise un logiciel ERP (Enterprise Resource Planning) afin de gérer son fichier clients. Le logiciel ERP prévoit des champs libres pour enregistrer des informations supplémentaires sur la relation avec le client et pour faciliter le suivi de dossier. N'enregistrez pas d'informations excessives dans ces champs libres ! Dans le cas d'un retard de paiement, l'indication de certaines raisons telles que "*le client est séparé*" ou "*le client est sans emploi*" n'est pas pertinente ;
- une PME qui engage une personne doit connaître un certain nombre de données en matière de sécurité sociale, situation familiale, diplômes obtenus. L'employeur peut exclusivement conserver les données qui sont nécessaires à la relation professionnelle avec le travailleur. La PME ne peut donc pas conserver des données médicales, comme par exemple le fait que le travailleur a souffert cette année-là d'une pneumonie et qu'il a été victime d'une fracture de la jambe. La PME peut toutefois consigner le nombre de jours pendant lesquels le travailleur a été absent pour cause de maladie.

TO DO

Triez les données traitées et posez-vous toujours la question de savoir s'il est encore réellement nécessaire de traiter ces données. Vous pouvez peut-être atteindre le même objectif avec moins de données ou avec des données moins sensibles.

Pour de plus amples informations

❖ Article 5.1.c) du RGPD – Principes relatifs au traitement des données à caractère personnel

1.5. Délai de conservation

Une PME ne peut jamais conserver des données à caractère personnel plus longtemps que le temps nécessaire à la réalisation des finalités envisagées. Dès que ces finalités sont accomplies ou disparaissent, une PME doit effacer les données à caractère personnel. En effet, à défaut d'une finalité, la nécessité de conserver et de traiter les données disparaît. Dès lors, une PME doit définir un délai de conservation maximal pour toutes ses données à caractère personnel. Parfois, le législateur lui-même a déjà défini un délai de conservation obligatoire.

o **EXEMPLE:**

- une PME ne doit effacer les données à caractère personnel reprises dans la comptabilité qu'après sept ans. L'article III.88 du Code de droit économique prévoit que les entreprises sont tenues de conserver leurs livres pendant 7 ans. Le même raisonnement s'applique aux documents, tels que les factures, que la PME doit conserver en vertu de la législation TVA ou pour les impôts directs ;
- une PME doit supprimer les données à caractère personnel d'un candidat dès qu'il est clair que la personne concernée ne sera pas engagée. (Supposons que la PME veuille quand même conserver ces informations, elle doit en informer le candidat et lui donner la possibilité de s'y opposer) ;
- une PME licencie un membre du personnel. La PME peut archiver le dossier du personnel et le conserver aussi longtemps que court le délai de prescription pour une éventuelle défense de droits en justice ou que la législation sociale le prescrit. Par la suite, la PME n'a toutefois plus aucune raison d'encore conserver plus longtemps ces données à caractère personnel et doit les effacer ;
- un bureau de chasseurs de têtes collecte les C.V. de demandeurs d'emploi afin de les associer à un employeur intéressé. Le bureau conserve ces C.V. pendant dix ans. Cette période est disproportionnée par rapport à la finalité qui consiste à trouver un emploi pour le demandeur d'emploi à court terme.

Instaurez une politique de conservation avec un accès différencié. Le traitement de dossiers en cours requiert une conservation permettant aux données d'être normalement disponibles et accessibles pour le gestionnaire de dossier. Dès qu'un dossier peut être archivé, la PME doit opter pour un mode de conservation ne conférant aux données qu'une disponibilité et une accessibilité limitées. Cette deuxième méthode de conservation est légitime, vu les finalités de la conservation ultérieure, comme le respect des dispositions légales en matière de prescription ou de délais de conservation obligatoires. Lorsque cette conservation n'est plus utile non plus, les données doivent être effacées.

TO DO

Établissez un inventaire du délai de conservation de toutes les données à caractère personnel que vous traitez et motivez toujours les raisons pour lesquelles vous avez encore besoin de ces données. Instaurez également une politique de conservation avec un accès différencié.

Pour de plus amples informations

- ❖ Article 5.1.e) du RGPD – Principes relatifs au traitement des données à caractère personnel

1.6 Transparence

Sans les informations nécessaires relatives à leurs droits, aux tenants et aboutissants de l'activité de traitement, les personnes concernées ne peuvent pas exercer leurs droits. C'est pourquoi une communication transparente est cruciale. En tant que responsable du traitement, la PME doit mener une communication *proactive* de manière à ce que les personnes concernées sachent précisément qui traite les données à caractère personnel, pour quelles raisons et à qui elles peuvent s'adresser en cas de problème.

La transparence est une obligation générale qui a des conséquences à trois niveaux. Tout d'abord, la PME a l'obligation d'informer la personne concernée de manière proactive. Deuxièmement, la transparence oblige le responsable du traitement à faciliter l'exercice des droits des personnes concernées (voir ci-après titre III Droits de la personne concernée). Enfin, la transparence a des conséquences sur *la manière de communiquer*. En tant que responsable du traitement, la PME a l'obligation de rédiger toutes les communications relatives au traitement de données à caractère personnel en des termes clairs et compréhensibles qui sont adaptés au public cible. En outre, ces informations doivent être aisément accessibles. Cela signifie que la personne concernée doit immédiatement savoir clairement où elle peut trouver les informations nécessaires.

o EXEMPLE:

- une politique en matière de protection de la vie privée sur le site Internet d'une PME ne peut pas contenir de langage trop juridique, ni utiliser des tournures inutilement complexes ;
- le lien Internet vers la politique en matière de protection de la vie privée doit être clairement visible sur le site Internet de la PME. La couleur et une position qui accroche le regard peuvent y contribuer ;
- des phrases comme «*Nous pouvons utiliser vos données afin de développer de nouveaux services*» ou «*Nous pouvons utiliser vos données afin de proposer des services personnalisés*» ne sont pas transparentes car on ne sait pas clairement quels services sont développés ou ce que «personnalisés» implique précisément.

Lisez également titre III.1 Le droit à l'information/l'obligation d'informer afin d'obtenir davantage de renseignements sur la transparence dans le contexte du droit à l'information et sur l'obligation d'une information proactive lors de la collecte de données à caractère personnel.

TO DO

Veillez à communiquer de manière transparente à l'égard des clients, du personnel et des fournisseurs quant au traitement de leurs données à caractère personnel. Formulez les informations en des termes adaptés au groupe cible (par ex. les enfants).

Pour de plus amples informations

- ❖ Article 5.1.a) du RGPD – Principes relatifs au traitement des données à caractère personnel
- ❖ Article 12 du RGPD – Information transparente
- ❖ Articles 13 et 14 du RGPD- Informations à fournir
- ❖ Lignes directrices du Groupe 29 sur la transparence en vertu du Règlement 2016/679- WP260

1.7. Sécurité

Chaque PME doit prendre des mesures techniques et organisationnelles appropriées pour garantir la sécurité des données à caractère personnel. Ces mesures sont aussi bien organisationnelles que techniques- acquérir un progiciel de sécurité prêt à l'emploi ne suffit donc pas toujours ! La PME doit protéger les données à caractère personnel contre un accès ou un traitement non autorisés, la perte et les dégâts.

La mise en œuvre concrète de cette obligation peut varier en fonction des risques et de la portée du traitement, du coût et de la faisabilité technique. Le RGPD n'exige donc pas nécessairement qu'une petite PME fournisse le fin du fin en matière de sécurité de l'information. Vous trouverez ci-dessous quelques exemples de mesures de protection organisationnelles (1.7.1) et techniques (1.7.2).

Pour de plus amples informations
❖ Article 5.1.f) du RGPD – Principes relatifs au traitement des données à caractère personnel
❖ Article 32 du RGPD- Sécurité du traitement
❖ Cybersécurité- Guide pour la PME du Centre for Cyber Security Belgium
❖ Directives de l'ENISA pour les PME sur le traitement sûr de données à caractère personnel

1.7.1. Mesures organisationnelles

1.7.1.1. Sensibilisation et formation :

Sensibilisez l'ensemble du personnel afin de les familiariser avec les principes de base en matière de protection des données. En particulier les membres du personnel ayant accès aux données à caractère personnel proprement dites doivent être formés de manière à ce qu'ils n'abusent pas (in)consciemment de cet accès. Cette mesure accessible à tous doit être mise en œuvre par chaque PME.

1.7.1.2. Définissez une politique de sécurité :

Cela signifie que la direction de la PME conçoit et met en œuvre une politique explicite. Cette politique comprend au moins les points suivants :

- mettre sur pied des procédures à l'arrivée et au départ des utilisateurs ;
- diffuser un code de conduite général pour l'utilisation ICT ;
- désigner un responsable en sécurité de l'information ;
- organiser régulièrement des audits de sécurité et les exécuter loyalement ;
- concevoir une politique d'accès qui accorde exclusivement un accès à des données à caractère personnel sur une base de "need-to-know" (besoin d'en connaître) ;
- établir des procédures internes afin de traiter les plaintes et de réagir de manière adéquate à des incidents (par ex. une fuite de données).

1.7.2. Mesures techniques

Plusieurs mesures accessibles à tous peuvent être déployées simplement dans l'infrastructure IT de la plupart des PME, comme :

- utiliser un antivirus et le mettre à jour systématiquement et en temps opportun ;
- réaliser systématiquement un back-up afin de se protéger contre la perte ;
- mettre à jour systématiquement et automatiquement tous vos logiciels ;
- faire fonctionner votre site Internet via une connexion https sécurisée ;
- installer un firewall" (tant pour le matériel que pour le logiciel) ;
- garantir la sécurité physique des serveurs en autorisant uniquement le personnel habilité (par ex. à l'aide de badges) ;
- instaurer un système d'accès avec un identifiant unique (login) pour chaque utilisateur et un mécanisme d'authentification.

2 Mesures de protection adaptées aux risques

Le RGPD accorde aux droits de la personne concernée une place centrale et entend dès lors identifier et limiter les risques liés à un traitement. Le RGPD aide les PME à réaliser cette analyse des risques nécessaire et propose plusieurs moyens pour faciliter ce processus. De plus, ces mesures contribuent à garantir de manière proactive le respect du RGPD. Dans le présent chapitre, nous passons en revue les différentes étapes :

- Étape 1 : le registre des activités de traitement- répertorier les traitements ;
- Étape 2 : désigner un délégué à la protection des données (DPO) ;
- Étape 3 : réaliser une analyse d›impact relative à la protection des données (AIPD).

Une PME ne doit procéder aux étapes 2 et 3 que si certaines conditions sont remplies. En cas de doute, il est préférable que la PME documente les raisons pour lesquelles elle a estimé que ces étapes n'étaient pas nécessaires.

2.1 Étape 1 : Établir un relevé à l›aide du registre des activités de traitement

Établir un relevé de toutes les activités de traitement de données à caractère personnel constitue une étape indispensable dans l'évaluation du risque. Le RGPD impose à chaque responsable du traitement ainsi qu'à chaque sous-traitant de conserver une documentation interne des activités de traitement qui ont lieu sous leur responsabilité. Ce registre leur permet d'avoir une idée des opérations de traitement qu'ils effectuent. Ce registre doit être fait par écrit (par voie électronique ou sur papier) et doit être clair et compréhensible.

Le registre contient un relevé des activités de traitement et pas des données à caractère personnel proprement dites. Le registre doit au moins mentionner les informations suivantes :

- ***Qui*** : le nom et les coordonnées du responsable du traitement et du délégué à la protection des données (DPO) ;
- ***Pourquoi*** : le registre mentionne, par traitement, les finalités du traitement en détail ;
- ***Quoi***: le registre mentionne, par traitement, les types de données à caractère personnel et de personnes concernées ;
- ***Où*** : le registre mentionne tous les destinataires des données à caractère personnel, les transferts vers un pays en dehors de l'Union européenne et les éventuelles garanties appropriées en cas d'un tel transfert ;
- ***Délai de conservation*** : dans la mesure du possible, le délai prévu pour l'effacement des données à caractère personnel ;
- ***Sécurité*** : dans la mesure du possible, une description générale des mesures de sécurité.

Le registre joue un rôle crucial dans le respect du RGPD. Il s'agit d'un outil fondamental pour pouvoir remplir de nombreuses autres obligations telles que l'information des personnes concernées et la gestion efficace des demandes visant à exercer leurs droits (comme l'accès, la rectification et l'effacement). Toutefois, le RGPD prévoit une exception pour les PME. La portée de cette exception est cependant très limitée :

- une organisation de moins de 250 personnes en service ne doit pas tenir de registre ;
- *sauf si* :
  - le traitement de données à caractère personnel n'est pas occasionnel ; *ou*
  - le traitement comporte un risque pour les droits et libertés des personnes concernées ; *ou*
  - le traitement concerne des données sensibles.

Vous trouverez ci-dessous une brève explication de ces situations dans lesquelles une PME doit quand même tenir un registre :

- **si le traitement est habituel (n'est pas occasionnel)** : occasionnel signifie que le traitement de données à caractère personnel n'a pas lieu systématiquement au sein de la PME. Si le traitement s'inscrit dans le cadre du fonctionnement normal de la PME, cette dernière devra tenir un registre, au moins pour ce traitement. Au sein d'une PME, les traitements liés à la gestion de la clientèle, du personnel (ressources humaines) et des fournisseurs par exemple ne sont pas occasionnels.

  o **EXEMPLE** : une entreprise de plomberie de vingt membres du personnel doit tenir un registre pour les traitements de données à caractère personnel de ses clients, de son personnel et de ses fournisseurs (pour autant qu'il ne s'agisse pas d'une personne morale dans ce dernier cas).

- **le traitement comporte un risque pour les droits et libertés des personnes concernées** : il s'agit d'une disposition générale qui entend prévenir le contournement de l'approche basée sur les risques. Le considérant 75 du RGPD énumère quelques situations dans lesquelles il est question d'un tel risque : un dommage financier ou social, le profilage, l'impossibilité pour la personne concernée d'exercer ses droits, la quantité de données à caractère personnel, le nombre de personnes concernées et le traitement de données de personnes vulnérables (par ex. des enfants).

  o **EXEMPLE** : une crèche qui enregistre les données des enfants accueillis doit constituer un registre à cet effet.

- **le traitement de données sensibles** : le traitement de certaines données sensibles engendre un risque plus élevé d'abus ultérieur.

  - **EXEMPLE** : un cabinet de médecins généralistes qui traite des données médicales de ses patients doit constituer un registre.

En résumé, cela signifie que l'obligation de tenir un registre ne disparaît que dans un nombre très limité de situations. C'est précisément pour cette raison que nous recommandons à tous les responsables du traitement et à tous les sous-traitants de tenir un registre, même si cela n'est pas strictement obligatoire. Pour une PME ayant un nombre limité de traitements de données, il ne s'agit pas d'une tâche insurmontable. En outre, la constitution de ce registre est indispensable pour réaliser une estimation correcte des obligations qui découlent du RGPD.

Nous encourageons les fédérations sectorielles à élaborer des modèles comportant les éléments communs que les PME peuvent reprendre dans leur registre.

TO DO

Établissez un registre des activités de traitement - à cet effet, vous pouvez utiliser les outils suivants :
1) le modèle de registre établi par la Commission vie privée ; et
2) la notice explicative pour la déclaration préalable que la Commission vie privée a élaborée. Bien que l'obligation d'une déclaration préalable disparaisse, cette déclaration contient de nombreuses informations utiles qui doivent également figurer dans le registre. Cette notice explicative contient une liste des finalités fréquentes qui peut aider les PME à compléter leur registre.

Pour de plus amples informations

- Article 30 du RGPD- Registre des activités de traitement
- Recommandation n° 06/2017 de la Commission vie privée sur le registre
- Schéma de la Commission vie privée : "Dois-je tenir un registre ?"
- FAQ de la Commission vie privée sur le Registre des activités de traitement

2.2 Étape 2 : Désigner un délégué à la protection des données (DPO)

Certains responsables du traitement et sous-traitants doivent désigner un délégué à la protection des données (Data Protection Officer ou DPO). Le délégué à la protection des données a pour mission :

- d'informer et d'émettre des avis pour respecter le RGPD ;
- d'émettre des avis sur demande concernant l'AIPD ;
- de contrôler si les traitements respectent le RGPD ;
- d'intervenir en tant que point de contact pour l'autorité de contrôle.

2.2.1. Dois-je désigner un délégué à la protection des données ?

Toutes les PME ne devront pas désigner un délégué à la protection des données. La désignation est **obligatoire** dans trois cas :

- une autorité publique effectue le traitement ; ou
- *les activités de base* de la PME consistent en une observation à grande échelle et systématique des personnes concernées ;

  - **EXEMPLE** : la géolocalisation via une application mobile, le profilage et l'observation au moyen de caméras de surveillance sont des exemples possibles d'observation systématique.

- ou *les activités de base* de la PME consistent en un traitement à grande échelle de données sensibles.

Les notions d' "*activités de base*" et d' "à grande échelle" sont cruciales pour déterminer si une PME doit désigner un DPO. "Activités de base" signifie que le traitement découle des activités principales de la PME et pas d'une activité secondaire de pur appui, telle que le paiement du personnel ou le support IT. "À grande échelle" peut aussi bien se rapporter au volume de données, au nombre de personnes concernées, à la durée ou à la couverture géographique et ne se réduit pas simplement à un chiffre déterminé.

o **EXEMPLE :**

- à titre d›activité principale, une PME collecte et combine des données à caractère personnel de plusieurs sources afin d›établir des profils de clients et d›ensuite les revendre à des publicitaires. Ce profilage est une forme d›observation systématique. Au final, il faudra évaluer *concrètement* si le traitement est à grande échelle ou pas. Si tel est le cas, la désignation d'un DPO est nécessaire ;
- une PME installe une caméra de surveillance orientée sur la caisse du magasin. Le fait de filmer entraîne une observation systématique de personnes physiques. Le traitement n'est toutefois pas à grande échelle et filmer pour des finalités de sécurité ne constitue pas une activité principale de la PME. Dans ce cas, la PME ne doit pas désigner de DPO ;
- une PME gère un site Internet permettant à des hôpitaux d'échanger des informations médicales avec des médecins généralistes de toute la province. L'activité principale de la PME consiste à échanger des données sensibles. Le développement régional de ce site Internet est à échelle suffisamment grande pour obliger la désignation d'un DPO.

Vous pouvez d'ailleurs toujours désigner un délégué à la protection des données **sur une base volontaire**, même si ce n'est pas juridiquement obligatoire. Attention : si vous désignez un délégué à la protection des données sur une base volontaire, vous devez respecter toutes les règles du RGPD relatives aux tâches et à la position du délégué à la protection des données. Soyez donc attentif à une utilisation irréfléchie du titre de fonction DPO ou délégué à la protection des données ! N'utilisez ce titre que s'il s'agit d'un véritable délégué à la protection des données au sens du RGPD.

2.2.2. La position du délégué à la protection des données

La PME doit aider le délégué à la protection des données en lui fournissant un accès aux données à caractère personnel et aux traitements. Les ressources nécessaires doivent également être mises à disposition pour qu'il puisse remplir ses missions (temps, formation, équipement et moyens financiers). Le délégué à la protection des données doit avoir accès à la haute direction afin de cartographier les problèmes.

Le délégué à la protection des données doit également être indépendant. Cela signifie que la PME :

- ne peut pas donner d'instructions au délégué à la protection des données en ce qui concerne l'exercice de ses missions ;
- ne peut pas pénaliser ou relever de ses fonctions le délégué à la protection des données pour l'exercice de ses missions.

Afin de garantir l'indépendance, le délégué à la protection des données ne peut assumer d'autres missions ou fonctions que si ces responsabilités supplémentaires ne conduisent pas à un conflit d'intérêts. Cela implique que le délégué à la protection des données ne peut pas avoir une position dans laquelle il détermine les finalités et les moyens du traitement de données à caractère personnel. Les fonctions conflictuelles comprennent surtout des postes de direction (chef RH, chef IT, administrateur délégué) mais peuvent également concerner des fonctions inférieures.

Le RGPD prévoit la possibilité de désigner un délégué externe à la protection des données dans le cadre d'un contrat de prestation de services.

TO DO

1) Vérifiez si vous devez désigner un délégué à la protection des données et, en cas de doute, **documentez** les raisons pour lesquelles vous désignez/ne désignez pas un DPO.
2) Vérifiez si votre délégué à la protection des données n'assume pas d'autres missions qui compromettent l'indépendance de sa position (conflit d'intérêts).
3) Même si vous ne désignez pas un véritable DPO, nous vous conseillons de désigner une personne qui contrôle le respect du RGPD et intervient en tant que personne de contact pour les personnes concernées qui exercent leurs droits. Ne donnez pas à cette personne le titre de "DPO" ou de "délégué à la protection des données" !

Pour de plus amples informations

- Articles 37-39 du RGPD – Délégué à la protection des données
- Lignes directrices du Groupe 29 concernant les délégués à la protection des données (DPD) – WP243
- Recommandation n° 04/2017 de la Commission vie privée relative au délégué à la protection des données
- Schéma de la Commission vie privée : "Dois-je tenir un registre ?"
- FAQ de la Commission vie privée sur le délégué à la protection des données

2.3 Étape 3 : Réaliser une analyse d›impact relative à la protection des données (AIPD)

L'AIPD est un processus continu servant à détecter, évaluer et finalement contrôler les risques pour les droits et libertés de personnes physiques. L'AIPD n'est obligatoire que lorsque le traitement implique un **risque élevé** pour les droits et libertés de personnes physiques. Le Groupe 29 a établi une liste de neuf facteurs qui contribuent à évaluer quand il y a un risque élevé (voir le cadre 'Pour de plus amples informations'). Plus il y a de facteurs présents dans le traitement, plus grande est la probabilité qu'il soit question d'un traitement comportant un risque élevé. Vous devez évaluer au cas par cas si le risque est élevé et si une AIPD est donc nécessaire.

La PME doit procéder à une AIPD avant le début du traitement et doit répéter cette analyse régulièrement de manière à ce que l'évaluation des risques et les mesures y afférentes restent d'actualité. Une AIPD comprend au moins :

- une description détaillée et claire des opérations de traitement envisagées et des finalités ;
- une évaluation de la proportionnalité des opérations de traitement au regard des finalités ;
- une évaluation des risques pour les droits et libertés des personnes concernées ;
- les mesures envisagées pour faire face aux risques.

o **EXEMPLE :**

- une PME observe les habitudes de navigation de son personnel afin de prévenir un usage privé excessif pendant les heures de travail. Dans ce cas, il s'agit d'une observation systématique et d'une évaluation. En outre, les travailleurs se trouvent dans une position subalterne- donc vulnérable- vis-à-vis de l'employeur. Dans ce cas, le risque est élevé et une AIPD est très probablement nécessaire.

L'APD établira également à l›avenir une liste des types d›opérations de traitement pour lesquelles une AIPD est automatiquement obligatoire. Dans un certain nombre de cas, le RGPD lui-même estime que le risque est élevé par définition et que vous devez quoi qu'il en soit procéder à une AIPD :

- **lors de l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, y compris le profilage,** si cela conduit à des décisions qui affectent de manière significative la personne concernée ;
    - o **EXEMPLE** : la PME utilise une plateforme de recrutement en ligne qui sélectionne et rejette automatiquement des candidats sur la base d'une lecture automatique du C.V.
- **dans le cadre du traitement à grande échelle de données à caractère personnel sensibles** au sens des articles 9 et 10 du RGPD ;
    - o **EXEMPLE** :une start-up développe une application de santé sur la base d'une plateforme ouverte (par ex. Android) qui collecte des données sur le sommeil, les habitudes alimentaires et l'activité physique.
- dans le cadre de la **surveillance** systématique à grande échelle d'une zone accessible au public.

Parfois, les mesures que vous prenez dans le cadre de l'AIPD ne suffisent pas pour limiter suffisamment le risque élevé. Si après la réalisation de l'AIPD, le risque résiduel- qui est le risque qui subsiste malgré les mesures que vous prenez dans le cadre de l'AIPD- reste toujours élevé, vous devez recueillir l'avis de l'APD.

TO DO

Évaluez la nécessité de procéder à une AIPD :
1) vous trouvez-vous dans un des trois cas qui requièrent une AIPD ?
2) si non, la PME opère-t-elle des traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques ?
3) si non, une AIPD n'est pas nécessaire mais la PME **devra justifier et documenter sa décision** .

Pour de plus amples informations

- ❖ Articles 35-36 du RGPD – Analyse d'impact relative à la protection des données
- ❖ Lignes directrices du Groupe 29 concernant l'analyse d'impact relative à la protection des données – Groupe 248
- ❖ Recommandation de la Commission vie privée concernant l'analyse d'impact relative à la protection des données
- ❖ Schéma de la Commission vie privée : "Dois-je tenir un registre ?"
- ❖ FAQ de la Commission vie privée concernant l'analyse d'impact relative à la protection des données

3 Prestataires de services externes

Afin d'épargner des frais pour l'installation d'une infrastructure IT autonome, des PME ont souvent recours à des prestataires de services externes - des sous-traitants donc - pour stocker des données à caractère personnel ou pour obtenir certains services (outsourcing).

- **EXEMPLE** : une brasserie locale fait appel à un secrétariat social pour gérer l'administration des salaires. La brasserie communique les détails du paiement comme le moment, les augmentations salariales ou un licenciement. Le secrétariat social utilise sa propre infrastructure IT pour enregistrer les données du personnel et assurer l'administration des salaires. Le secrétariat social est le sous-traitant et la brasserie est le responsable du traitement.

Recourir à un prestataire de services externe est autorisé mais doit toujours s'accompagner de plusieurs garanties. Ces garanties doivent faire en sorte que la PME conserve un contrôle suffisant sur ce qu'il advient des données à caractère personnel et que ces dernières restent bien sécurisées. L'enregistrement et le traitement de données dans le cloud sont des formes courantes d'outsourcing. Dans le choix du Cloud Service Provider (CSP, fournisseur de services cloud), la PME devra notamment tenir compte de la sécurité des données à caractère personnel échangées. Le déséquilibre des forces dans la relation contractuelle ne dispense pas la PME de sa responsabilité d'accepter uniquement des conditions contractuelles qui soient conformes au RGPD.

Vous trouverez ci-dessous les mesures que vous devez prendre si vous avez recours à un prestataire de services externe :

3.1 Concluez un contrat

3.1.1. Procédez à une sélection scrupuleuse

Les PME ne peuvent recourir qu'à des sous-traitants qui offrent *des garanties suffisantes* afin que le traitement réponde aux exigences du RGPD et que les droits des personnes concernées restent garantis. Les garanties doivent notamment concerner la sécurité et l'application de mesures *techniques et organisationnelles appropriées* (voir notamment le titre II.1.7 Sécurité).

3.1.2. Concluez un contrat écrit

Lorsque le traitement de données à caractère personnel est confié à un sous-traitant, les deux parties doivent conclure un "contrat de sous-traitance". Ce contrat doit établir explicitement que le prestataire de services peut traiter les données à caractère personnel *exclusivement sur la base des instructions écrites* de la PME. Le contrat doit au moins contenir les éléments suivants :

- l'objet et la durée du contrat, les finalités et la nature du traitement, le type de données, les catégories de personnes concernées et les droits et obligations des deux parties ;
- le sous-traitant garantit qu'il ne traitera les données à caractère personnel que sur la base des instructions écrites de la PME et qu'il ne les utilisera pas pour quelque autre finalité (sauf obligation légale explicite) ;
- le sous-traitant garantit qu'il prendra les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque ;
- le sous-traitant promet qu'il ne recrutera aucun autre sous-traitant sans l'autorisation écrite préalable de la PME. Si le sous-traitant recrute quand même un sous-traitant, il doit imposer à ce dernier toutes les obligations qui découlent du premier contrat de sous-traitance entre la PME et le premier sous-traitant ;
- le sous-traitant garantit que les personnes habilitées par lui à traiter les données à caractère personnel (par ex. des techniciens chargés de la gestion du service) se sont engagées à respecter la confidentialité ou sont tenues par une obligation légale de confidentialité appropriée ;
- le sous-traitant est d'accord d'aider, dans toute la mesure du possible, la PME à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées la saisissent en vue d'exercer leurs droits ;
- le sous-traitant se déclare disposé à aider, le cas échéant, la PME à garantir le respect de ses obligations en matière de sécurité, de notification et/ou communication d'une violation de données à caractère personnel ou d'AIPD ;

– les données ne sont pas transmises en dehors de l'Union européenne vers des destinations n'offrant pas un niveau de protection adéquat ou sans garanties appropriées supplémentaires qui seront convenues au préalable avec la PME ;

– le sous-traitant garantit qu'au terme de la prestation de services, toutes les données à caractère personnel seront supprimées en toute sécurité ou renvoyées à la PME et que les copies existantes seront détruites ;

– le sous-traitant est d'accord de mettre à la disposition de la PME toutes les informations nécessaires pour démontrer le respect de ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par la PME ou par un autre contrôleur qu'elle a mandaté, et de contribuer à ces audits.

3.1.3. Contrôlez le respect des accords

La PME doit veiller à ce que le prestataire de services externe respecte effectivement les accords conclus. C'est la raison pour laquelle le contrat de sous-traitance doit aussi établir que le prestataire de services doit mettre à la disposition de la PME toutes les informations nécessaires pour démontrer le respect de ses obligations.

TO DO

1) Évaluez les contrats actuels et futurs avec des prestataires de services externes et apportez-y les changements nécessaires en temps opportun (donc avant le 25 mai 2018). Dans ce cadre, tenez compte des éléments minimaux prescrits par l'article 28 du RGPD, dont l'engagement selon lequel les données à caractère personnel qui sont confiées ne peuvent être traitées que sur la base des instructions écrites de la PME ;
2) Vérifiez que les prestataires de services tant actuels que futurs offrent des garanties suffisantes, en particulier en ce qui concerne la sécurité des données à caractère personnel ;
3) Réclamez en temps voulu les informations nécessaires qui démontrent que le prestataire de services respecte ses obligations.

Pour de plus amples informations

❖ Article 28 du RGPD- Sous-traitant
❖ Article 29 du RGPD- Traitement effectué sous l'autorité du responsable du traitement ou du sous-traitant
❖ Avis 05/2012 du Groupe 29 sur l'informatique en nuage – WP196
❖ Avis n° 10/2016 de la Commission vie privée relatif au recours au cloud computing par les responsables du traitement.

4 Où vont vos données ?

Parfois, une PME obtient des données à caractère personnel en Belgique mais pour le traitement ultérieur de ces données, elle fait appel aux services d'un sous-traitant dont les serveurs se trouvent à l'étranger. Au sein de l'Union européenne, toutes les données à caractère personnel peuvent circuler librement. Si le traitement de données a lieu en Allemagne par exemple, la PME ne doit pas exiger de garanties supplémentaires. Si le traitement de données a lieu en dehors de l'Union européenne, le transfert des données à caractère personnel ne peut se faire que sous des conditions strictes.

Le transfert vers un «pays tiers» en dehors de l'Union européenne est autorisé :

- lorsque cette destination est reconnue par la Commission européenne comme étant une destination offrant un niveau de protection similaire (décision d'adéquation). La liste des destinations reconnues est disponible sur ce site Internet;
- lorsque le sous-traitant offre des garanties appropriées supplémentaires dans le contrat pour assurer un niveau de protection similaire de manière contractuelle. Cela est possible en ajoutant des dispositions type que la Commission européenne ou l'APD a approuvées ;

Ces mécanismes garantissent la sécurité des données à caractère personnel et veillent à ce que les personnes concernées puissent exercer leurs droits, même si le traitement a lieu dans un pays ayant un autre type de législation en matière de protection de la vie privée.

Le RGPD prévoit encore plusieurs autres mécanismes afin de permettre des transferts vers un pays tiers (des règles d'entreprise contraignantes, des codes de conduite, des dérogations pour des situations spécifiques, etc.). Ceux-ci

dépassent toutefois le cadre de la présente brochure. Il importe surtout qu'une PME sache où vont ses données et qu'elle comprenne qu'un transfert en dehors de l'Union européenne exige des garanties supplémentaires.

- **EXEMPLE** : une PME a recours à un sous-traitant suisse pour gérer le trafic de courriers électroniques (fournir des adresses e-mail, enregistrer les courriers électroniques, etc.). Le soustraitant conserve les courriers électroniques sur des serveurs qui se trouvent en Suisse. Ce transfert de données à caractère personnel n'exige pas de garanties complémentaires car la Suisse est reconnue par la Commission européenne comme une destination offrant un niveau de protection similaire.

TO DO

Contrôlez si votre sous-traitant traite les données à caractère personnel en dehors de l'Union européenne.
1) Si oui, contrôlez alors si cette destination est reprise dans la liste de destinations présentant un niveau de protection adéquat qui ont été reconnues par la Commission européenne.
2) Si la destination ne figure pas sur cette liste, vous devez négocier des garanties contractuelles supplémentaires.

Pour de plus amples informations

- ❖ Chapitre V du RGPD- Transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales
- ❖ Page Internet de la Commission européenne pour les "Data transfers outside the EU"

III. Droits de la personne concernée

Outre l'imposition de certaines obligations qui ont été abordées ci-dessus, le RGPD prévoit des droits que chaque personne concernée peut exercer. La personne concernée exerce ces droits à l›égard du responsable du traitement. Le sous-traitant doit assister le responsable du traitement pour permettre l'exercice de ces droits. Il s'agit en particulier :

1. du droit à l'information/de l'obligation d'informer
1. du droit d'accès
3. du droit de rectification
4. du droit à l'effacement des données
5. du droit à la limitation du traitement des données
6. du droit d'opposition
7. du droit à la portabilité des données
8. du droit de ne pas faire l'objet d'une décision individuelle automatisée.

Attention : certains droits ne s'appliquent pas pour chaque base juridique (voir titre II.1.1. Base juridique) ! Lors de l'analyse de chaque droit, nous expliquons toujours en détail le lien entre la base juridique et le droit.

Dans l'exercice des droits des personnes concernées, la transparence joue également un rôle clé. Ainsi, le responsable du traitement doit :

- informer clairement la personne concernée sur l'existence de ces droits (titre III.1 Information) ;
- communiquer dans un langage compréhensible et clair si une personne concernée exerce ses droits ;
- faciliter l'exercice de ces droits, notamment via des moyens électroniques ;

- **EXEMPLE** : prévoyez sur votre site Internet un formulaire en ligne afin d'exercer le droit d'accès.

La PME ne peut réclamer **aucun paiement** pour l'exercice de ces droits. Vous pouvez toutefois exiger le paiement de frais si la demande de la personne concernée est clairement infondée ou excessive. Ces frais doivent être adaptés au coût administratif supporté par la PME pour donner suite à la demande. Vous devez évidemment pouvoir prouver que la demande est clairement infondée ou excessive.

Lorsque la personne concernée exerce un de ses droits, la PME doit y donner suite **dans un délai d'un mois**. S'il s'agit d'une demande complexe, la PME peut alors prolonger ce délai de deux mois après que la personne en a été informée dans un délai d'un mois. Si la PME peut prouver que la demande est clairement infondée ou excessive, elle peut ignorer la demande.

- **EXEMPLE** : un client assaille toutes les semaines une PME d'une dizaine de demandes pour exercer son droit d'accès, sans motif fondé. La PME peut ignorer la demande ou exiger le paiement de frais qui correspondent au coût administratif requis pour fournir une réponse.

Quand la PME ne donne pas suite à la demande concrète formulée par la personne concernée, elle doit informer cette dernière, dans un délai d'un mois à compter de la réception de la demande, des motifs de son inaction (par ex. pourquoi elle ne procède pas à l'effacement des données). En outre, la PME doit informer la personne concernée de la possibilité d'introduire une réclamation auprès de l'APD et de former un recours juridictionnel.

TO DO
Élaborez une procédure interne et désignez une personne de contact centrale qui peut donner suite dans un délai d'un mois aux demandes de personnes concernées d'exercer leurs droits.

Pour de plus amples informations
❖ Article 12 du RGPD – Modalités de l'exercice des droits de la personne concernée
❖ Lignes directrices du Groupe 29 sur la transparence en vertu du Règlement 2016/679- WP260

1 Le droit à l'information/l'obligation d'informer

Chaque personne concernée a droit à certaines informations lorsqu'une PME traite des données la concernant. La PME a l'obligation d'informer la personne concernée. Le RGPD fait une distinction entre la collecte directe de données à caractère personnel auprès de la personne concernée elle-même (collecte directe- article 13 du RGPD) et la situation où les données à caractère personnel ne sont pas obtenues auprès de la personne concernée elle-même mais auprès d›une autre source (collecte indirecte- article 14 du RGPD).

1.1 Quelles informations ?

Tant lors de la collecte directe que de la collecte indirecte de données à caractère personnel, une PME doit, en tant que responsable du traitement, fournir certaines informations à la personne concernée. Nous parcourons ci-dessous les informations de base que la PME doit communiquer à la personne concernée, tant lors d'une collecte directe que lors d'une collecte indirecte :

Information	Directe	Indirecte
les **finalités** et la **base juridique** du traitement	✓	✓
les données d'identité et de contact du **responsable du traitement** et du **DPO** (s'il y a un DPO)	✓	✓
les **destinataires** ou les catégories de destinataires des données ;	✓	✓
lors de **transferts en dehors de l'Union Européenne** : l'existence d'une décision d'adéquation ou de garanties appropriées et la manière dont vous pouvez en obtenir une copie	✓	✓
des explications sur **l'intérêt légitime** du responsable du traitement si le traitement repose sur cette base juridique	✓	
les catégories de **données** traitées		✓

En outre, le RGPD prescrit qu'une PME doit fournir les informations suivantes afin de garantir un traitement équitable et transparent. Les lignes directrices du Groupe 29 sur la transparence définissent quand vous devez communiquer ces informations (voir de plus amples informations en page 31) :

Information	Directe	Indirecte
le délai de conservation ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer ce délai	✓	✓
le droit d'accès, d'effacement, de rectification, de limitation, d'opposition et le droit à la portabilité	✓	✓
le droit d'introduire une réclamation auprès d'une autorité de contrôle	✓	✓
si le traitement se fonde sur le consentement : le droit de retirer son consentement à tout moment	✓	✓

Information	Directe	Indirecte
l'existence d'une prise de décision automatisée, les informations utiles concernant la logique sous-jacente et les conséquences prévues de ce traitement pour la personne concernée	✓	✓
des explications sur l'intérêt légitime du responsable du traitement si le traitement repose sur cette base juridique		✓
la source des données		✓
si la personne concernée est obligée de fournir les données à caractère personnel (par la loi ou par un contrat) et quelles sont les conséquences en cas de refus de fournir ces données	✓	

Le responsable du traitement doit à nouveau communiquer les informations susmentionnées de ce deuxième tableau en cas de traitement ultérieur pour une nouvelle finalité compatible qui diffère de la finalité initiale (voir le titre II.1.2 Finalité). Dans ce cas, la PME doit également fournir à la personne concernée des informations sur l'analyse qui prouve que la nouvelle et l'ancienne finalité sont compatibles.

1.2 Quand les informations doivent-elles être fournies ?

En cas de collecte directe, la PME doit communiquer les informations au moment de la collecte des données à caractère personnel. En cas de collecte indirecte de données à caractère personnel, la PME doit fournir les informations au plus tard dans un délai d'un mois après l'obtention initiale des données à caractère personnel. Ce délai maximal d'un mois est réduit- jamais prolongé- :

- si les données à caractère personnel sont utilisées aux fins de la communication avec la personne concernée. La PME informe alors au plus tard au moment de la première communication à ladite personne ;
- si les données sont transmises à un autre destinataire. La PME informe alors au plus tard lorsque les données à caractère personnel sont communiquées.

Par souci de clarté : si le transfert ou la première communication a lieu au-delà d'un mois après l'obtention initiale des données à caractère personnel, la PME doit simplement communiquer les informations dans le mois qui suit l'obtention initiale.

Lors de toute modification ultérieure apportée au traitement (par ex. de nouveaux destinataires, une finalité compatible, un transfert en dehors de l'Union européenne, etc.), la PME doit en informer la personne concernée largement à l'avance. Plus la modification est substantielle, plus tôt la PME doit en informer la personne concernée de manière à ce que cette dernière dispose d'un délai raisonnable pour en apprécier l'impact et exercer ses droits.

1.3 Quand la PME ne doit-elle pas communiquer d'informations ?

La PME ne doit pas communiquer les informations si la personne concernée les a déjà reçues. En cas de collecte indirecte de données à caractère personnel, des exceptions supplémentaires sont d'application. Ainsi, la communication des informations n'est pas nécessaire si :

- la fourniture de telles informations se révèle impossible ou exigerait des efforts disproportionnés. La barre pour cette exception est toutefois placée très haut, ce qui implique qu'un responsable du traitement ne peut invoquer ces situations qu'exceptionnellement ; *ou*
- l'obtention ou la communication des données sont expressément prévues par la loi ;
    - **EXEMPLE** : la loi oblige le fisc à réclamer certaines informations sur un travailleur auprès de l'employeur. Le fisc ne doit pas informer le travailleur lui-même. Dans le cadre de son obligation d'information, l'employeur informera le travailleur du fait que le fisc est un des destinataires des données à caractère personnel.
- *ou* les données à caractère personnel doivent rester confidentielles en vertu d'une obligation légale de secret professionnel.

1.4 Comment les informations doivent-elles être communiquées ?

Nous recommandons **de fournir les informations par couche**. Cela permet d'éviter qu'un excès d'informations nuise à la transparence et que la personne concernée se noie dans une abondance d'informations. La communication des informations par couche concilie l'exigence de concision avec celle de fournir toutes les informations nécessaires. Cela simplifie non seulement la mission du responsable du traitement mais permet aussi à la personne concernée d'intégrer rapidement et efficacement les informations essentielles. Afin de veiller à une communication loyale des informations, la présentation de ces informations pourrait être la suivante :

- une première couche avec *des informations de base*.
    - QUOI ? : la PME fournit un résumé des informations de base nécessaires dont la personne concernée a besoin pour évaluer l'impact et la portée du traitement (par ex. : l'identité du responsable du traitement, les finalités, les catégories de destinataires, la source des données, ...).
    - COMMENT ? : sous forme de tableau, à un endroit clairement visible avec le titre «Informations de base sur la protection des données» ou via des pop-ups qui fournissent les explications lors de la collecte des données à caractère personnel. Si le traitement repose sur le consentement, il est préférable que vous mentionniez ces informations à l'endroit où la personne concernée doit donner son accord (près du bouton «d'accord»).
- une deuxième couche avec *des informations complémentaires* détaillées.
    - QUOI ? : cette partie présente de manière compréhensible et générale les autres informations que la PME doit communiquer en vertu des articles 13 et 14 du RGPD.
    - COMMENT ?: : les informations complémentaires peuvent être fournies de plusieurs manières, par ex. au moyen d'hyperliens au départ des informations de base ou d'un chargement via une URL. Les informations complémentaires doivent trouver un équilibre entre concision et précision. Les informations doivent être structurées de manière à être facilement lisibles.

TO DO

Adaptez votre site Internet et vos conditions générales de manière à ce que :
1) votre politique en matière de protection de la vie privée soit clairement visible et mentionne toutes les informations des articles 13/14 du RGPD ;
2) vos pages Internet d'enregistrement et de transaction conduisent, par couche, à toutes les informations des articles 13/14 du RGPD.

Pour de plus amples informations

- Article 13 du RGPD – Collecte directe
- Article 14 du RGPD – Collecte indirecte
- Lignes directrices du Groupe 29 sur la transparence en vertu du Règlement 2016/679- WP260

2 Le droit d'accès

Le droit d'accès permet à la personne concernée de contrôler la licéité de chaque activité de traitement. Le droit d'accès comporte trois volets :

1) La personne concernée a le droit de savoir si la PME traite ou non ses données à caractère personnel.

2) Si oui, la personne concernée a le droit d'obtenir les informations mentionnées ci-dessous :

- les *finalités* du traitement ;
- les *catégories de données à caractère personnel* ;
- les *destinataires ou les catégories de destinataires* des données à caractère personnel ;
- le *délai de conservation* des données à caractère personnel ou les critères utilisés pour déterminer ce délai ;
- l'existence du *droit* à l'effacement, à la rectification des données à caractère personnel et du droit de limiter le traitement ou de s'y opposer ;
- l'existence du droit d'introduire une réclamation auprès d'une autorité de contrôle ;
- la *source* des données (en cas de collecte indirecte) ;

- lors d'un transfert *en dehors de l'Union Européenne* : les garanties appropriées (par ex. des dispositions types - voir titre II.4 Où vont vos données);
- l'existence d'une *prise de décision automatisée*, les informations utiles concernant la logique sous-jacente et les conséquences prévues de ce traitement pour la personne concernée.

3) La personne concernée a le droit d'obtenir gratuitement une copie de ses données à caractère personnel que la PME traite. Si la personne concernée demande des copies supplémentaires, la PME peut exiger le paiement de frais raisonnables qui ne sont pas supérieurs au coût administratif de ces copies. Lorsque la personne concernée présente sa demande par voie électronique, la PME communique les informations dans un format électronique d'usage courant, à moins que la personne concernée ne demande une copie sur un autre support physique (par ex. sur papier). Avant de communiquer la copie, la PME doit vérifier si cette communication ne porte pas préjudice aux droits et libertés d'autres personnes concernées (par ex. si des informations relatives à plus d'une personne sont traitées dans un même fichier).

- **EXEMPLE :**
  - un membre du personnel de la PME demande un accès à son dossier du personnel et veut en obtenir une copie gratuitement. La PME fournit une copie du dossier du personnel avec une note explicative du traitement (voir le point 2) ci-dessus).

Pour de plus amples informations
❖ Article 13 du RGPD – Droit d'accès de la personne concernée

3 Le droit de rectification

La personne concernée a le droit de rectifier des données inexactes ou de compléter des données incomplètes, y compris en fournissant une déclaration complémentaire. Si la PME a transmis ces données à caractère personnel à des tiers, elle doit les informer de la rectification qui a été apportée, à moins que cela se révèle impossible ou exige des efforts disproportionnés.

- **EXEMPLE** : un client informe une PME qu'il a déménagé. La PME doit adapter l'adresse dans son fichier clients.

Pour de plus amples informations
❖ Article 16 du RGPD- Droit de rectification
❖ Article 19 du RGPD- Obligation de notification en ce qui concerne la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement

4 Le droit à l'effacement des données

Une personne concernée peut exiger que la PME efface des données à caractère personnel pour lesquelles il n'y a plus de motif fondé de les traiter. Le droit d'effacer des données n'est pas absolu. La personne concernée ne peut exercer ce droit que dans les cas suivants :

- les données à caractère personnel ne sont plus nécessaires à la réalisation de la **finalité** poursuivie ;
- la PME traite les données à caractère personnel de manière **illicite**;
- la PME doit effacer les données à caractère personnel en raison d'une **obligation légale** ;
- la personne concernée **retire son consentement** et le traitement n'a pas d'autre base juridique ;
- après l'exercice réussi du droit d'**opposition** (voir le titre III.6 Droit d'opposition);
- des **mineurs** qui ont donné leur consentement pour utiliser un service en ligne peuvent toujours demander l'effacement de ces données à caractère personnel (quel que soit leur âge actuel).

Avez-vous transmis auparavant les données effacées à quelqu'un d'autre ? La PME doit alors informer ces destinataires de l'effacement des données, à moins que cela se révèle impossible ou exige des efforts disproportionnés.

- **EXEMPLE** : une personne concernée s'inscrit sur un site de réseau social. La personne concernée décide de quitter le site de réseau social et demande à la société de supprimer toutes les données à caractère personnel. La société doit donner suite à cette requête.

La PME peut également refuser d'effacer les données à caractère personnel lorsque le traitement est notamment nécessaire pour :

- l'exercice du droit à la liberté d'expression et d'information;
- la constatation, l'exercice ou la défense d'un droit en justice ;
- le respect d'une obligation légale à laquelle la PME est soumise ou l'exécution d'une mission d'intérêt général dont est investie la PME ;
- la recherche, les statistiques, la santé publique, l'archivage dans l'intérêt public- sous des conditions spécifiques.

o **EXEMPLE** : un membre du personnel qui vient d'être licencié demande que ses données à caractère personnel soient effacées de son dossier du personnel. La PME est toutefois légalement obligée de conserver plusieurs documents sociaux (registre du personnel, compte individuel, copie des états de salaire, etc.) pendant cinq ans. Pour ces documents, la PME doit refuser la demande d'effacement des données.

Pour de plus amples informations

- ❖ Article 17 du RGPD- Droit à l'effacement
- ❖ Article 19 du RGPD- Obligation de notification en ce qui concerne la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement

5 Le droit à la limitation du traitement de données

Dans certaines circonstances, la personne concernée peut exiger une "limitation" du traitement de données. La limitation gèle le traitement de données. Dès lors, la PME peut encore uniquement conserver les données à caractère personnel et doit cesser toutes les autres activités de traitement.

La personne concernée a le droit d'obtenir la limitation du traitement de données lorsque :

- elle conteste **l'exactitude** des données à caractère personnel pendant une durée permettant à la PME de vérifier l'exactitude des données à caractère personnel ;
- le traitement est **illicite** : plutôt que l'effacement des données, la personne concernée peut demander la limitation de l'utilisation des données à caractère personnel ;
- la PME n'a plus besoin des données à caractère personnel mais celles-ci sont encore nécessaires à la personne concernée pour l'exercice d'un **droit en justice** ;
- la personne concernée exerce son droit d'**opposition**. La limitation s'applique le temps de vérifier si les motifs légitimes poursuivis par la PME prévalent sur ceux de la personne concernée.

Si la personne concernée exerce son droit à la limitation avec succès, la PME ne peut encore utiliser les données qu'avec le consentement de la personne concernée ou pour intenter une action en justice[5]. Avez-vous transmis auparavant les données 'gelées' à quelqu'un d'autre ? Vous devez alors informer ces destinataires de la limitation du traitement, à moins que cela se révèle impossible ou exige des efforts disproportionnés.

Pour de plus amples informations

- ❖ Article 18 du RGPD- Le droit à la limitation du traitement
- ❖ Article 19 du RGPD- Obligation de notification en ce qui concerne la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement

6 Le droit d'opposition

Chaque personne concernée peut s'opposer au traitement de données à caractère personnel la concernant "*pour des raisons tenant à sa situation particulière*". Le droit d'opposition peut exclusivement être exercé si le traitement repose sur une des bases juridiques suivantes :

- l'intérêt légitime de la PME ou d'un tiers ;
- l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique.

5 Les données peuvent encore être traitées pour la protection des droits d'une autre personne physique ou morale, ou pour des motifs importants d'intérêt public de l'Union ou d'un État membre (article 18(2) du RGPD).

Dans les autres cas, la personne concernée ne peut pas s'opposer car il existe pour les autres bases juridiques des alternatives pour atteindre la même finalité : en cas de consentement, la personne concernée peut le retirer ; la personne concernée ne peut pas s'opposer au traitement imposé par la loi.

L'exercice du droit d'opposition contraint la PME à procéder à une mise en balance des intérêts. La PME cesse tout traitement des données à caractère personnel à moins qu'elle puisse avancer des motifs impérieux qui prévalent sur les droits et libertés de la personne concernée (par ex. une action en justice). La PME doit documenter et communiquer ces motifs à la personne concernée.

⚠ Une exception importante à cette mise en balance des intérêts existe en faveur de la personne concernée : en cas de **marketing direct**, la personne concernée a toujours le droit de s'opposer sans la moindre motivation. Cette opposition conduit donc automatiquement à l'arrêt du traitement pour cette finalité.

⚠ La PME doit attirer l'attention de la personne concernée, de manière claire et distincte d'une autre information, sur la possibilité d'exercer le droit d'opposition. Par ex. au moyen d'un bouton bien visible.

- **EXEMPLE :**

  - la personne concernée achète en ligne un ticket pour le concert d'un groupe. Par la suite, la personne concernée reçoit des publicités pour des concerts et des événements. La personne concernée souhaite ne plus recevoir ces publicités et s'y oppose. La PME doit mettre fin au marketing direct ;
  - dans le secteur des assurances, des données à caractère personnel sont nécessaires dans certaines situations pour lutter contre les pratiques de blanchiment d'argent. Dès lors, il arrive qu'un courtier d'assurances refuse de donner suite à une opposition car la législation antiblanchiment l'oblige à conserver les données.

Pour de plus amples informations

❖ Article 21 du RGPD- Droit d'opposition

7 Le droit à la portabilité des données

Le droit à la portabilité des données permet à la personne concernée d'obtenir ses données à caractère personnel et de les réutiliser pour d'autres services. La personne concernée peut, de manière conviviale, déplacer ses données à caractère personnel d'un environnement IT vers un autre.

Le droit à la portabilité des données peut uniquement être exercé lorsque trois conditions sont remplies simultanément :

✓ le traitement a lieu sur la base du consentement ou d'un contrat ;

✓ il s'agit d'un traitement automatisé (donc pas de documents papier) ; *et*

✓ la personne concernée fournit elle-même les données. Cela signifie que ce droit concerne uniquement les données à caractère personnel :

- que la personne concernée a elle-même fournies consciemment (par ex. lors d'un enregistrement : nom, adresse, etc.) ;
- que la PME observe sur la base du comportement de la personne concernée (par ex. les accessoires connectés) ;
- ce droit ne concerne pas des données que la PME crée elle-même sur la base des données susmentionnées.

La personne concernée a le droit :

- d'obtenir ses données à caractère personnel dans un format structuré, couramment utilisé et lisible par machine. Le format doit permettre à la personne concernée de réutiliser les données à caractère personnel pour un autre service ;

  - **EXEMPLE** : XML, JSON et CSV sont des formats courants qui répondent à ce critère. Des métadonnées doivent également être transmises de manière à ce que les données puissent fonctionner sur une autre plateforme. Un format PDF ne suffit pas.

- de faire directement transférer ses données à caractère personnel vers un autre responsable du traitement. La PME ne doit le faire que dans la mesure où un tel transfert direct est techniquement possible.

- **EXEMPLE :**
  - un consommateur peut demander le transfert de sa liste de chansons d'un service de streaming musical en ligne ;
  - une PME qui propose un service de webmail doit transférer la liste d'adresses et les e-mails de la personne concernée à un autre service de webmail à condition que cela soit techniquement possible. Si cela n'est pas possible, la PME fournit la liste d'adresses à la personne concernée dans un format numérique courant et réutilisable.

Pour de plus amples informations

- Article 20 du RGPD- Droit à la portabilité des données
- Lignes directrices du Groupe 29 sur le droit à la portabilité des données- WP242

8 Le droit de ne pas être soumis à une décision individuelle automatisée

Une personne concernée ne peut pas faire l'objet d'une décision entièrement automatique- sans intervention humaine - qui l'affecte de manière significative ou qui a des effets juridiques.

Le profilage peut parfois aller de pair avec une décision automatisée. Le profilage renvoie à : "*toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique*" (article 4, (4) du RGPD).

Afin d'invoquer cette interdiction, il doit s'agir :

- d'une décision qui repose exclusivement sur un traitement automatisé, sans intervention humaine. Cela signifie qu'une personne physique n'exerce aucun contrôle significatif sur la décision et ne peut par exemple pas modifier ou annuler la décision ;

- d'une décision qui entraîne des effets juridiques pour la personne concernée ou qui l'affecte de manière significative.

  - **EXEMPLE** : *effets juridiques* : la résiliation automatique d'un contrat de téléphonie parce que le client n'a pas payé la facture mensuelle.

  - **EXEMPLE** : *affecte de manière significative* : dans les cas ci-dessous, la décision *peut* affecter la personne concernée de manière significative, mais cela dépend toujours du contexte :

    - le refus automatique d'un crédit de paiement pour un achat en ligne ;
    - le refus automatique de candidats qui postulent via une plateforme en ligne ;
    - une différenciation de prix sur la base des habitudes de navigation et d'achat d'un consommateur.

Dans trois situations, on peut quand même appliquer la décision individuelle automatisée :

- si une loi l'autorise (par exemple la prévention de la fraude ou de l'évasion fiscale) ;
- si la décision est fondée sur un consentement explicite de la personne concernée ; ou
- si cela est nécessaire à la conclusion ou à l'exécution d'un contrat.
  - Attention : cette dernière situation dépend toujours d'une évaluation concrète. Dès que des méthodes portant moins atteinte à la vie privée existent pour conclure ou exécuter le contrat, la mesure n'est plus 'nécessaire'.

Si une PME applique une décision automatisée dans un de ces trois cas, elle doit prévoir des mesures appropriées qui protègent les droits de la personne concernée. Ces mesures comprennent au moins la possibilité pour la personne concernée de contester cette décision, d'exprimer son point de vue et de demander une intervention humaine.

⚠ En cas de données sensibles, la décision automatisée n'est possible que sur la base d'un consentement explicite ou d'un intérêt public important en vertu de droit de l'Union ou du droit national.

Pour de plus amples informations

- Article 22 du RGPD- Décision individuelle automatisée, y compris le profilage
- Lignes directrices du Groupe 29 sur la décision individuelle automatisée

IV. Que faire si les choses tournent mal ?

1. Une fuite de données - documentez-la et notifiez-la !

Chaque PME doit instaurer des procédures pour notifier certaines violations de données à caractère personnel (également appelées “data breaches”). Le RGPD définit une fuite de données comme étant une violation de la sécurité entraînant, de manière accidentelle ou intentionnelle, la destruction, la perte, l’altération ou la transmission non autorisée de données à caractère personnel ou l’accès non autorisé à de telles données. Une fuite de données arrive plus facilement qu’on ne le pense :

o **EXEMPLE** : des exemples de fuites de données sont :

- une cyberattaque dans laquelle un ransomware bloque l’accès à l’infrastructure IT ;
- un ordinateur portable professionnel, une clé USB ou un CD contenant des données à caractère personnel perdu(e) ou volé(e) ;
- une importante coupure de courant qui a pour conséquence que l’accès aux serveurs est indisponible.

La PME doit consigner chaque fuite de données- même la plus petite- dans un **journal interne**. Ce journal mentionne : la cause, les données à caractère personnel affectées, les conséquences et les mesures prises. En outre, il convient de conseiller de reprendre aussi dans ce journal la raison pour laquelle on n’a pas notifié une fuite de données. Ce journal peut être intégré dans le registre des activités de traitement.

En outre, la PME doit également **notifier** la fuite de données dans certaines situations:

- **à l›APD :** si la fuite de données est susceptible d’engendrer **un risque pour les** droits et libertés de la personne concernée ;
- **à la personne concernée :** si la fuite de données est susceptible d’engendrer **un risque élevé** pour les droits et libertés de la personne concernée.

1.1 Notification à l’APD

Une PME doit notifier une fuite de données à l’APD si celle-ci est susceptible d’engendrer **un risque** pour les droits et libertés de la personne concernée.

Si la PME est responsable du traitement, la notification doit se faire dans un délai de 72 heures après que la PME a été informée de la fuite de données. La PME peut ainsi d’abord vérifier une notification d’un client concernant une possible fuite de données avant d’être officiellement informée et que le délai de 72 heures commence. Si la PME est un sous-traitant, elle notifie immédiatement la fuite de données au responsable du traitement.

La notification mentionne au minimum : le moment de la fuite de données, le moment auquel la PME en a été informée, la cause probable, les données à caractère personnel affectées, les conséquences, les mesures prises et les coordonnées de la personne qui assure le suivi de la fuite de données au sein de la PME. La PME qui est au courant d’une fuite de données mais ne dispose pas encore de toutes ces informations peut déjà procéder à la notification et fournir ultérieurement les autres informations.

o EXEMPLE :

- lors d’une effraction, un CD crypté contenant des données du personnel est volé. La PME dispose d’une sauvegarde des données. Tant que la clé de cryptage n’est pas volée ou craquée, une notification n’est pas nécessaire, en l’absence de risque ;
- une PME ayant une boutique en ligne reçoit une notification d’un client qui a reçu un mail suspect l’invitant à payer une facture. La PME constate, au terme d’une courte enquête, qu’un tiers intercepte systématiquement ses données clients. À présent, la PME est au courant de la fuite de données et elle la notifie dans les 72 heures à l’APD et à ses clients qui ont été affectés.

1.2 Notification à la personne concernée

Une PME doit notifier une fuite de données aux individus affectés si celle-ci est susceptible d’engendrer **un risque élevé** pour les droits et libertés de la personne concernée. Ce n’est toutefois pas nécessaire si :

- la PME avait prévu des mesures de sécurité à appliquer en cas de fuite de données, comme par exemple une méthode de cryptage forte ;
- la PME a pris des mesures après la fuite de données faisant en sorte que le risque élevé n'est plus susceptible de se matérialiser (par ex. l'effacement à distance en cas de vol du support) ;
- la communication individuelle exigerait des efforts disproportionnés. Une communication publique est recommandée dans ce cas afin d'informer les personnes concernées.

o **EXEMPLE :**

  – une PME collecte, au moyen d'accessoires connectés, des données sur le sommeil, les habitudes alimentaires et l'activité physique et en déduit des informations relatives à la santé. La transmission de ces données se révèle non sécurisée et des hackers ont publié en ligne les données brutes, avec les profils d'utilisateurs. Dans ce cas, le risque est suffisamment élevé pour informer non seulement l'APD mais également les utilisateurs ;
  – un hacker a accès aux données du personnel d'une société de marketing. L'intrusion est détectée. Les données concernées sont l'adresse, la composition de ménage, le salaire et les congés de maladie. La société informe l'APD dans les 72 heures et informe également le personnel.

1.3 Quand y a-t-il un risque (élevé) ?

Les critères suivants sont pertinents pour déterminer s'il est question d'un risque (élevé) probable en cas de fuite de données. Cette liste n'est pas exhaustive et dans la pratique, la PME devra toujours procéder à une évaluation effective en fonction du cas concret. C'est précisément pour cette raison qu'il est important d'également reprendre dans le journal des fuites de données à caractère personnel le motif de la non-notification.

- la sensibilité des données ayant fait l'objet de la fuite : par ex. des données relatives à la situation financière, à la santé, à des documents d'identité ;
- la quantité des données ayant fait l'objet de la fuite : certaines données peuvent être inoffensives prises séparément mais pas lorsqu'elles sont combinées ;
- les conséquences possibles pour un individu : vol d'identité, fraude, atteinte à la réputation ou humiliation ;
- le nombre d'individus affectés ;
- la vulnérabilité des individus : données à caractère personnel d'enfants, de personnes âgées ou de personnes handicapées ;
- la facilité à identifier les individus : les données ont-elles été cryptées ou codées ?

Pour de plus amples informations

❖ Articles 33-34 du RGPD – Notification d'une violation de données à caractère personnel
❖ Lignes directrices du Groupe 29 concernant la notification d'une violation de données à caractère personnel en vertu du Règlement 2016/679- WP250

2 Une violation du RGPD

En cas de violation du RGPD, la personne concernée peut invoquer deux mécanismes coercitifs parallèles. La personne concernée qui pense que le traitement de ses données à caractère personnel enfreint le RGPD peut adresser à l'APD une réclamation qui peut aboutir à une sanction pour la PME, ou exiger une réparation via le tribunal ordinaire. Rien n'exclut que les personnes concernées introduisent simultanément une réclamation auprès de l'APD et s'adressent au juge.

2.1 Sanctions

L'APD peut imposer différentes sanctions en cas de non-respect du RGPD. Dans le cadre d'une réclamation ou de sa propre initiative, l'APD peut notamment :

- donner un avertissement ou formuler un rappel à l'ordre ;
- obliger à satisfaire à la demande de la personne concernée ;
- obliger à mettre le traitement en conformité avec le RGPD dans un délai déterminé ;
- geler ou interdire le traitement ;
- infliger des amendes jusqu'à 2 % ou 4 % du chiffre d'affaires annuel, en fonction de la violation.

La PME a une obligation de coopérer en cas d'enquête éventuelle de l'APD (article 31 du RGPD). Si une personne concernée ou la PME n'est pas d'accord avec une décision juridiquement contraignante de l'APD qui lui est adressée, elle peut former un recours juridictionnel contre cette décision (article 78 du RGPD).

2.2 Réparation

Chaque personne qui subit un dommage en raison d'une violation du RGPD peut exiger réparation devant le tribunal (article 79 du RGPD).

Si plusieurs responsables du traitement et/ou sous-traitants participent à un même traitement, la personne concernée peut aussi bien s'adresser aux responsables du traitement qu'aux sous-traitants (article 82 du RGPD). Chacun des responsables du traitement ou des sous-traitants impliqués est tenu responsable du dommage dans sa totalité à l'égard de l'individu affecté, à moins qu'il puisse prouver qu'il n'est en aucune manière responsable du dommage subi.

Après la réparation totale vis-à-vis de l'individu concerné, le responsable du traitement et le soustraitant peuvent exercer un recours mutuel. Le responsable du traitement ou le sous-traitant qui a réparé totalement le dommage subi est en droit de réclamer auprès des autres responsables du traitement ou sous-traitants ayant participé au même traitement la part de la réparation correspondant à leur part de responsabilité dans le dommage.

Attention donc : même si le problème se situe au niveau de votre sous-traitant, la personne concernée peut directement s'adresser à vous qui êtes responsable du traitement !

- **EXEMPLE** : une PME établie en Belgique enregistre des données sensibles de clients auprès d'un centre de données. Une fuite de données survient au centre de données, affectant les données clients de la PME. Le client peut s'adresser à la PME belge afin d'obtenir réparation. Par la suite, la PME peut se retourner contre le centre de données pour récupérer une partie de la réparation payée.

Pour de plus amples informations

- Chapitre VIII du RGPD- Voies de recours, responsabilité et sanctions
- Lignes directrices du Groupe 29 sur le calcul et l'imposition d'amendes administratives en vertu du Règlement 2016/679- WP253

V. Check-list pour le sous-traitant

Les principales obligations s'appliquant au sous-traitant sont :

- ✓ Concluez **un contrat sans faille** avec le responsable du traitement Il s'agit d'une obligation. Voir le titre II.3.1 Concluez un contrat pour un contenu minimal de ce contrat. En tant que sous-traitant, vous ne pouvez pas utiliser les données à caractère personnel pour des finalités qui ne sont pas reprises dans ce contrat. Si vous le faites quand même, vous êtes considéré vous-même comme responsable du traitement pour ces nouvelles finalités.
- ✓ Travaillez-vous vous-même avec des **sous-traitants** ? C'est évidemment permis mais tenez compte du fait que le responsable du traitement doit marquer son accord au préalable.
- ✓ La **sécurité** est une obligation extrêmement importante pour un sous-traitant. Le sous-traitant aussi doit prendre des mesures techniques et organisationnelles pour garantir un traitement sûr des données à caractère personnel. Voir le titre II.1.7 Sécurité pour des exemples de mesures de sécurité appropriées.
- ✓ Conservez-vous ou transférez-vous des données à caractère personnel **en dehors de l'Union européenne** ? Notifiez-le au responsable du traitement et vérifiez si vous pouvez invoquer un des mécanismes pour le transfert de données à caractère personnel en dehors de l'Union européenne (voir le titre II.4 Où vont vos données ?).
- ✓ L'obligation de tenir un registre des activités de traitement s'applique de la même manière aux sous-traitants qu'aux responsables du traitement (voir le titre II.2.1 Étape 1 : Établir un relevé du registre des activités de traitement).

- ✓ Les sous-traitants doivent vérifier eux-mêmes s'ils doivent ou non désigner un DPO. Le fait que le responsable du traitement ne désigne pas de DPO ne signifie pas que le sous-traitant ne doit pas désigner de DPO non plus (voir le titre II.2.2 Étape 2. Désigner un délégué à la protection des données (DPO)).

- ✓ L'obligation de procéder à une AIPD incombe en premier lieu au responsable du traitement. Le sous-traitant doit toutefois assister le responsable du traitement dans l'exécution de l'AIPD.

- ✓ Les obligations liées à la tenue d'un journal et à la notification de **violations de données à caractère personnel** s'adressent d'abord aux responsables du traitement. Le sous-traitant doit assister le responsable du traitement dans le respect de ces obligations et doit notifier la violation de données à caractère personnel au responsable du traitement dans les meilleurs délais (voir le titre IV.1 Une fuite de données).

- ✓ Outre imposer des obligations, le RGPD attribue des **droits** à chaque personne concernée (voir le titre III Droits de la personne concernée). Pour l'exercice de ces droits, la personne concernée s'adresse au responsable du traitement. Le sous-traitant doit toutefois assister le responsable du traitement pour permettre l'exercice de ces droits.

- ✓ Une **obligation de coopération** incombe également au sous-traitant à l'égard de l'APD.

- ✓ Enfin, le sous-traitant doit **aussi assister le responsable du traitement** pour le respect de plusieurs obligations par ce dernier :

  - la sécurité du traitement par le responsable du traitement ;
  - l'exercice des droits par les personnes concernées (voir ci-dessus) ;
  - la journalisation et l'obligation de notification pour les violations de données à caractère personnel (voir ci-dessus) ;
  - l'exécution d'une AIPD par le responsable du traitement ;
  - la fourniture d'informations à l'APD lors d'une consultation préalable dans le cadre de l'AIPD.