Els Kindt - Pauline Hellemans

CiTiP, KU Leuven

26 juillet 2020

BROCHURE FAQ POUR PME

Projet BOOST - Booster la connaissance et le respect du RGPD chez les PME belges, en se concentrant sur trois thèmes principaux

Autorité de protection des données
Gegevensbeschermingsautoriteit

UNIVERSITÉ DE NAMUR

VUB VRIJE UNIVERSITEIT BRUSSEL

KU LEUVEN

Ce projet est financé par le programme Droits, Egalité et Citoyenneté REC-AG-2019 de l'Union européenne.

BROCHURE FAQ POUR PME

Els Kindt
CiTiP, KU Leuven

Pauline Hellemans
CiTiP, KU Leuven

26 juillet 2020

1. INTRODUCTION

La présente publication a été développée dans le cadre du projet BOOST (janvier – décembre 2020) et donne de plus amples explications sur l'application du Règlement général sur la protection des données (RGPD) et sur certaines de ses obligations. Elle est destinée aux petites et moyennes entreprises (PME) en Belgique et complète la précédente publication RGPD : vade-mecum pour les PME de l'Autorité de protection des données (APD). Elle précise certains aspects et obligations du RGPD, avec des exemples supplémentaires et des renvois vers des lignes directrices et des décisions récentes.

Cette brochure n'aborde pas le RGPD de manière exhaustive, mais se concentre sur quelques sujets importants. Ils ont été choisis sur la base de la description du projet BOOST et d'une consultation réalisée dans le cadre du projet BOOST au sujet des connaissances du RGPD et des problèmes actuels rencontrés par les PME. Nous aborderons les sujets suivants :

- les notions de « responsable du traitement » et de « sous-traitant »,
- le principe de transparence,
- l'analyse d'impact relative à la protection des données,
- le registre de traitement, et
- le Délégué à la protection des données (Data protection officer, DPO).

Ces sujets sont expliqués sous forme de questions et réponses.

Ce projet a été sponsorisé par le programme Droits, Egalité et Citoyenneté REC-AG-2019 de l'Union Européenne, sous la convention de subvention numéro 874505.

QU'EST-CE QUE LE RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES ?

Le Règlement général sur la protection des données (ci-après **RGPD**), parfois également appelé **GDPR**, est une législation de l'Union européenne. Vous trouverez le RGPD en intégralité ici.

Le RGPD impose des obligations pour **protéger** les « **données à caractère personnel** » et faire respecter les **droits fondamentaux** des personnes dans l'UE, en permettant aussi la libre circulation des données à caractère personnel.

Le RGPD est **d'application depuis le 25 mai 2018** et a notamment été complété en Belgique par la loi du 30 juillet 2018 (ci-après la **Loi relative à la protection des données de 2018**). Vous pouvez consulter ici la Loi relative à la protection des données de 2018.

2. MON ENTREPRISE DOIT-ELLE RESPECTER LE RGPD ?

Toute entreprise, organisation, association ou personne qui « traite » des « données à caractère personnel » de manière automatisée ou dans des fichiers doit respecter le RGPD. Étant donné que le champ d'application du RGPD est large, en pratique, quasiment toutes les entreprises devront respecter le RGPD. Vous trouverez ici une vidéo qui détaille ce champ d'application.

Base légale : article 2, 1. du RGPD

Le RGPD s'applique non seulement aux entreprises, mais aussi aux organisations et aux associations (comme les ASBL). Lorsque l'on évoque dans cette brochure de FAQ la notion d' « entreprise », on vise également systématiquement les associations et les organisations.

Exemple 1 : dès qu'une entreprise réalise une des activités suivantes, pour son propre compte ou pour le compte d'un tiers, elle doit, en tant que responsable du traitement ou sous-traitant, respecter le RGPD :

- l'enregistrement et le traitement sur ordinateur de données de clients (par exemple des listes de clients et des données de facturation avec des noms de personnes et leurs adresses e-mail, ...) et/ou de fournisseurs (par exemple des listes de fournisseurs avec des noms de personnes) ou la conservation de ces données sur des fiches papier ordonnées ;

- la réception, en ligne ou hors ligne, l'enregistrement et l'utilisation sur ordinateur de données de travailleurs, comme des fiches de salaire ou des données de curriculum vitae de candidats travailleurs ; la réclamation et l'enregistrement en ligne de données RH de travailleurs auprès d'une entreprise de gestion des salaires ;

- la tenue d'un site Internet sur un propre serveur ou sur des plateformes de tiers (par exemple une page Facebook) avec mention ou collecte (par exemple via des cookies) de données à caractère personnel.

Exemple 2 : Une ASBL qui exerce par exemple les activités suivantes doit respecter le RGPD :

- la collecte des coordonnées de ses membres pour organiser des réunions ;
- la conservation de données de fournisseurs pour traiter des livraisons ;
- la conservation et l'utilisation de données relatives aux indemnisations de bénévoles pour le paiement de ces indemnisations ;
- la conservation de données des visiteurs des locaux de l'ASBL ou des activités organisées par celle-ci.

Le RGPD s'applique donc à toutes les entreprises, y compris les PME, qui traitent des données à caractère personnel. La **taille ou le type d'activités de l'entreprise ne sont en principe pas importants à cet égard**. Certes, pour les petites et moyennes entreprises, quelques exigences sont plus souples, en particulier en ce qui concerne surtout la désignation d'un **délégué à la protection des données**.

QUE SONT LES « DONNÉES À CARACTÈRE PERSONNEL »

Les données à caractère personnel sont toutes les données et les informations au sujet d'une **personne identifiée ou identifiable.** Il s'agit d'une notion **large**. Une personne est identifiable si les informations peuvent être reliées, par des « *efforts raisonnables* », à la personne et si elles peuvent donner lieu à son identification, directement (par exemple via son nom) ou indirectement (par exemple à l'aide d'un numéro de client). Pour cet examen du « caractère raisonnable », des éléments tant objectifs (temps requis et moyens techniques) que contextuels (qui peuvent donc varier d'un cas à l'autre) importent.

Base légale : Article 4, (1) du RGPD

Exemples de données à caractère personnel : nom de famille, adresse e-mail, adresse, numéro de Registre national, préférences, adresse IP, habitudes de navigation et de clic sur un site Internet, données de localisation obtenues par exemple via une application mobile sur un smartphone, photo d'un visage (par exemple une photo d'un intérimaire), images de caméras, certificat médical, évaluation d'un membre du personnel, extrait du casier judiciaire, fiche de salaire d'un travailleur, ...

Grâce aux évolutions technologiques, de nombreuses données qui **semblent anonymes ne le sont pas et sont quand même des données à caractère personnel**, car elles permettent quand même d'identifier des personnes physiques, par exemple en les combinant avec d'autres données à caractère personnel ou en raison de leur nature. Vous trouverez plus d'informations à ce sujet ici.

Exemple : Les données de localisation d'un smartphone sont des données à caractère personnel, même si elles semblent anonymes.

Pour plus de lignes directrices quant à l'interprétation de l'utilisation de données de localisation pour des applications de traçage, voir l'Avis 4/2020 du Comité européen de la protection des données (EDPB), page 7.

QU'ENTEND-ON PAR « TRAITEMENT » ?

Le traitement de données à caractère personnel signifie **toute opération (ou tout ensemble d'opérations) appliquée(s) à (un ensemble de) données à caractère personnel** (réalisée avec ou sans aide de systèmes automatisés). Il s'agit d'une notion **large.**

Base légale Article 4, (2) du RGPD

Exemples de traitements : la collecte, l'inventaire, 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 de données à caractère personnel.

3. SELON LE RGPD, SUIS-JE UN « RESPONSABLE DU TRAITEMENT » OU UN « SOUS-TRAITANT » ?

Le RGPD distingue deux rôles importants : celui de responsable du traitement et celui de soustraitant. Cette distinction est cruciale car le responsable du traitement doit respecter plus d'obligations et a plus de responsabilités que le sous-traitant.

QU'EST-CE QU'UN RESPONSABLE (CONJOINT) DU TRAITEMENT ?

Le responsable du traitement est l'entreprise ou l'entité qui **décide pourquoi ou dans quel but** des données à caractère personnel sont collectées et utilisées et **comment** ces données à caractère personnel sont traitées. Autrement dit, le responsable décide des **finalités et des moyens**.

Lorsque deux entreprises décident conjointement des moyens et des finalités, elles sont **responsables conjoints**. Lorsqu'elles prennent ces décisions séparément, elles sont chacune un responsable distinct. Les responsables conjoints doivent déterminer qui assumera les obligations à l'égard des personnes concernées et ils doivent aussi le porter à la connaissance des personnes concernées.

Base légale : Articles 4, (7) et 26 du RGPD

Pour plus de lignes directrices quant à l'interprétation des notions de « sous-traitant » et de « responsable », voir l'Avis 1/2010 du Groupe de travail « Article 29 » et les lignes directrices 07/2020 du Comité européen de la protection des données (EDPB).

Exemple 1 : Votre PME décide qu'un enregistrement est nécessaire pour accéder à votre site Internet et demande un nom et une adresse e-mail via une procédure d'enregistrement en ligne (*comment*). Vous utiliserez ces données pour envoyer des e-mails publicitaires (*pourquoi*). Votre PME est **responsable**.

Exemple 2 : Pour sa carte de fidélité, une boulangerie décide de collaborer avec une entreprise qui propose gratuitement un système de fidélisation et qui collecte à cet effet des données à caractère personnel de la clientèle de la boulangerie. Le boulanger intervient en tant que responsable du traitement pour les traitements que l'entreprise réalise pour gérer la carte de fidélité gratuite pour le compte du boulanger, et l'entreprise est le sous-traitant. Toutefois, si l'entreprise réutilise vos données client à de propres fins, par exemple pour améliorer son système de fidélisation, elle devient elle-même **aussi un responsable du traitement** et la boulangerie et l'entreprise de fidélisation sont **chacune séparément des responsables du traitement.**

Exemple 3 : Une entreprise de marketing collecte des adresses e-mail et des données de clic de visiteurs d'un site Internet pour le compte et selon les instructions d'une PME à des fins de marketing. L'entreprise de marketing réutilise cependant ces données et profils collectés pour les combiner avec d'autres données de clic d'autres sites Internet pour les revendre à d'autres clients. L'entreprise de marketing et la PME sont alors **chacune distinctement un responsable du traitement.**

Exemple 4 : Un bureau d'assurances décide d'utiliser une application de facturation proposée par une plateforme. Le bureau décide avec le fournisseur de la plateforme d'utiliser les données à caractère personnel à des fins publicitaires. Tant le bureau que le fournisseur de la plateforme interviennent en tant que **responsables conjoints** pour l'utilisation des données à caractère personnel à des fins publicitaires.

Exemple 5 : Un bureau d'assurances indépendant décide d'utiliser une application de facturation proposée par une plateforme. L'application de facturation établit des factures pour le bureau, sur instruction du bureau. Le bureau intervient en tant que **responsable** et le fournisseur d'application intervient en tant que **sous-traitant**.

QU'EST-CE QU'UN « SOUS-TRAITANT » ?

Le sous-traitant est une entreprise ou une autre entité qui traite des données à caractère personnel **uniquement et exclusivement pour le compte** et **sur instruction** d'une **autre entreprise**. À noter qu'un responsable du traitement qui désigne un sous-traitant doit signer un contrat de sous-traitance avec ce sous-traitant.

Base légale : Article 4, (8) et 28 du RGPD

Exemple 1 : L'entreprise de marketing Y collecte des adresses e-mail via des sites Internet de tiers, à la demande spéciale de l'entreprise X, pour les finalités exclusives et selon les instructions de l'entreprise X. L'entreprise de marketing Y intervient en tant que sous-traitant pour cette collecte.

Exemple 2 : Une entreprise de gestion des salaires traite des données à caractère personnel pour une PME. L'entreprise de gestion des salaires interviendra en tant que sous-traitant si elle traite les données à caractère personnel uniquement et exclusivement sur instruction de la PME. La PME détermine les finalités et les moyens du traitement de données et est à ce titre responsable du traitement.

Exemple 3 : Un développeur de sites Internet développe des sites Internet sur instruction d'une entreprise. Pour créer et entretenir ces sites Internet, le développeur enregistre des données de visiteurs sur instruction de cette entreprise. Si le développeur de sites Internet traite des données de visiteurs exclusivement pour l'entreprise, il interviendra en tant que sous-traitant. L'entreprise intervient alors en tant que responsable du traitement.

Exemple 4 : Une entreprise conserve les données de ses clients non pas sur des serveurs locaux mais dans le *cloud*, chez un hébergeur. Cet hébergeur interviendra en tant que sous-traitant s'il utilise ces données à des fins qui ne lui sont pas propres.

Pour plus de lignes directrices quant à l'interprétation des notions de « sous-traitant » et de « responsable », voir l'Avis 1/2010 du Groupe de travail « Article 29 » et les lignes directrices 07/2020 du Comité européen de la protection des données (EDPB).

ARRÊT *FASHION ID* DE LA CJUE

La Cour de justice de l'Union européenne (CJUE) a précisé la notion de « responsables conjoints du traitement » (article 26 du RGPD) dans l'arrêt « Fashion ID ». La CJUE a en effet déterminé qu'une entreprise de vente en ligne qui a intégré sur son site Internet le bouton « like » de Facebook (appelé aussi « third party plugin ») est responsable, conjointement avec Facebook, du traitement des données à caractère personnel des utilisateurs du site Internet. En l'occurrence, cette responsabilité commune est certes limitée à la collecte de données via le site Internet et à leur transfert vers Facebook.

Il en découle que chaque PME qui intègre de tels « plug-ins » sur son site Internet est responsable conjointement avec Facebook et est tenue, en accord avec Facebook :

- de fournir aux utilisateurs les informations requises sur les traitements de leurs données, de même que les traitements effectués par Facebook, et
- lorsqu'il est exigé, de recevoir le consentement des utilisateurs avant la collecte et la transmission des données.

Vous pouvez lire l'intégralité de l'arrêt de la CJUE ici

4. QUELLES OBLIGATIONS MON ENTREPRISE DOIT-ELLE RESPECTER EN VERTU DU RGPD ?

Le RGPD impose plusieurs obligations à toutes les entreprises qui traitent des données à caractère personnel, qu'elles soient un responsable ou un sous-traitant. Le respect du RGPD va donc plus loin que la seule rédaction d'une déclaration de confidentialité. Cette déclaration est expliquée plus en détail ci-après.

Le respect du RGPD nécessite donc de manière globale une **analyse proactive approfondie et toujours répétée** de tous les flux et processus liés aux données à caractère personnel au sein d'une entreprise et requiert ensuite des actions pour le respect de toutes les obligations légales, basées sur ces analyses et évaluations, en vertu du droit de protection des données. En outre, un responsable du traitement doit pouvoir **démontrer et prouver** à tout moment que les obligations ci-dessous sont respectées au sein de son entreprise.

Nous reprenons ci-après, **brièvement** et de manière générale, les principales obligations :

I. Les sept principes généraux (« imposés ») de l'article 5 du RGPD

1. Traiter les données à caractère personnel de manière **licite, loyale et transparente** ;

QU'EST-CE QU'UN TRAITEMENT LICITE ET QUELS SONT LES FONDEMENTS D'UN TRAITEMENT ?

Pour que les données à caractère personnel soient traitées de manière licite, il faut **au moins la présence d'un des fondements suivants du RGPD pour le traitement** (article 6 du RGPD) **(et pour les données à caractère personnel sensibles, il faut également un motif d'exception requis par l'article 9 du RGPD)** :

- la personne concernée a donné son consentement pour le traitement (voir également ici, p. 8) ;
- le traitement est *nécessaire* à l'**exécution d'un contrat** avec la personne concernée ou pour des mesures précontractuelles (voir également ici, p. 9) ;
- le traitement est *nécessaire* pour une **obligation légale** qui incombe au responsable du traitement (voir également ici, p. 9) ;
- le traitement est *nécessaire* à la sauvegarde des **intérêts vitaux** de la personne concernée ou d'une autre personne physique ;
- le traitement est *nécessaire* pour une **mission d'intérêt public** (comme par exemple la santé publique, la protection sociale et la gestion de services de soins de santé) ou pour une **tâche relevant de l'exercice de l'autorité publique** du responsable ;
- le traitement est *nécessaire* pour un **intérêt légitime** du responsable du traitement ou d'un tiers et les intérêts ou les droits fondamentaux de la personne concernée ne prévalent pas, en particulier lorsqu'il s'agit d'un enfant (voir également ici, p. 10).

2. Ne collecter des données à caractère personnel que pour des **finalités déterminées, explicites et légitimes** et ne les traiter que pour des finalités qui sont **compatibles** avec les finalités initiales (**limitation des finalités)** (voir également ici, p. 10) ;
3. Ne traiter que des données à caractère personnel qui sont **adéquates, pertinentes et nécessaires** pour les finalités (**minimisation des données**) (pour plus d'informations, voir ici, p. 12) ;
4. Les données à caractère personnel doivent être **exactes** et **actualisées** et, au besoin, elles doivent être effacées ou rectifiées moyennant des mesures raisonnables (voir ici pour plus d'informations, p. 11) ;
5. Ne conserver les données à caractère personnel que **pour une durée strictement nécessaire** et les anonymiser dès que possible (voir ici pour plus d'informations, p. 12) ;
6. Prendre les mesures techniques et organisationnelles adéquates pour assurer l'**intégrité et la confidentialité** ;
7. Le responsable doit pouvoir **démontrer** le respect des obligations précitées (**principe de responsabilité**).

II. Obligations spécifiques pour traiter des données à caractère personnel de manière sûre et appropriée

- Déterminer le **fondement du traitement** et le motif d'exception pour les **données à caractère personnel sensibles** ;
- **Obligation d'information** détaillée ;
- Tenir un **registre de traitement** (voir ici pour plus d'informations, p. 15) ;
- Prendre des mesures techniques et organisationnelles afin de **protéger** les données à caractère personnel de manière appropriée (voir ici pour plus d'informations, p. 13 et ici pour des lignes directrices concrètes) ;
- Conclure un **contrat de sous-traitance** avec les sous-traitants (voir ici pour plus d'informations, p. 19) ;
- Réaliser au besoin une **Analyse d'impact relative à la protection des données** (voir ici pour plus d'informations, p. 18) ;
- **Ne pas exporter** des données à caractère personnel provenant de l'Espace économique européen, sauf si des mesures appropriées ont été prises (voir ici pour plus d'informations, p. 20) ;
- **Notifier une fuite de donn**ées à l'APD et éventuellement aussi aux personnes concernées (voir ici pour plus d'informations, p. 29) ;
- Désigner au besoin un **Délégué à la protection des données** (DPO) (voir ici pour plus d'informations, p. 16).

III. Obligations spécifiques à l'égard de personnes concernées (articles 12-25 du RGPD)

- Transparence et **obligation d'information** détaillée à l'égard des personnes concernées (voir la question 5 et les questions suivantes ci-dessous).
- Respect des droits des personnes concernées, à savoir :
  - Droit d'accès ;
  - Droit de rectification et d'effacement des données (voir ici pour plus d'informations, p. 25) ;
  - Droit à la limitation du traitement de données (voir ici pour plus d'informations, p. 26) ;
  - Droit à la portabilité des données (voir ici pour plus d'informations, p. 27) ;
  - Droit d'opposition (voir ici pour plus d'informations, p. 26) ;
  - Droit de ne pas être soumis à une prise de décision automatisée (voir ici pour plus d'informations, p. 28).

5. QU'EST-CE QUE LE PRINCIPE DE TRANSPARENCE EN VERTU DU RGPD ET QUELLES INFORMATIONS DOIS-JE COMMUNIQUER ?

Le RGPD entend donner plus de contrôle aux personnes concernées en ce qui concerne le traitement de leurs données à caractère personnel. Un des instruments majeurs du contrôle est en premier lieu la transparence, qui inclut l'information de la ou des personnes concernées de toute utilisation et du traitement de ces données à caractère personnel.

Ce n'est que si l'utilisation de données à caractère personnel est « transparente » pour les personnes concernées qu'elles peuvent évaluer les risques éventuels et prendre des décisions au sujet de leurs données à caractère personnel.

Le RGPD oblige donc les responsables du traitement à fournir des informations aux personnes concernées au sujet de l'identité du responsable et des données à caractère personnel qu'ils collectent, comment ils les utilisent (par exemple aussi pour créer des profils, les suivre sur des sites Internet, ...) et à qui elles sont transmises, combien de temps elles sont conservées, etc. En outre, les personnes concernées ont divers droits, dont le droit de réclamer des informations au sujet du traitement de leurs données à caractère personnel et de les consulter (article 15 du RGPD) (voir également ci-après).

Base légale : articles 12 et suivants du RGPD

Pour plus d'informations, voir les lignes directrices sur la transparence du Groupe de travail « Article 29 ».

QUI SONT LES « PERSONNES CONCERNÉES » ?

Les personnes concernées sont les personnes individuelles dont vous traitez les données à caractère personnel. Les entreprises et les personnes décédées ne sont pas des personnes concernées

Base légale : Article 4, (1) du RGPD

Voici quelques **exemples** de personnes concernées : les travailleurs dont la fiche de salaire est établie, la personne dont une photo est enregistrée, les clients qui se trouvent sur un listing client, les titulaires d'un numéro de téléphone ou d'une adresse e-mail qui est utilisée à des fins de marketing, la personne dont les données de localisation sont enregistrées et/ou transférées, ...

6. QU'EST-CE QU'UNE « DÉCLARATION DE CONFIDENTIALITÉ » ?

En cas de *collecte directe* auprès des personnes concernées, les entreprises doivent leur communiquer des informations détaillées au sujet des traitements de manière **concise, transparente et compréhensible**, **aisément accessible** et ces informations doivent être **formulées en des termes clairs et simples**. Cela peut se faire par écrit (par exemple au verso d'un devis) ou par voie électronique (par exemple sur un site Internet). Si la personne concernée le demande, vous pouvez également transmettre ces informations verbalement, mais vous devez ensuite pouvoir le prouver.

Même en cas de *collecte indirecte*, donc si vous ne recevez **pas directement les données à caractère personnel d'une personne concernée**, mais par exemple via un tiers, vous

devez fournir les mêmes informations détaillées aux personnes concernées, mais en outre les catégories de données à caractère personnel et leur source, sauf si par exemple les personnes concernées disposent déjà des informations ou si cela se révèle impossible ou exige des efforts disproportionnés.

Exemple : Des données à caractère personnel achetées à un revendeur (*data broker*), collectées sur les médias sociaux, obtenues via une autre entreprise ou plateforme, ...

Base légale : Article 12 et Articles 13 et 14 du RGPD

Pour plus d'informations, voir les lignes directrices sur la transparence du Groupe de travail « Article 29 ».

QUELS CONSEILS CONCRETS PUIS-JE APPLIQUER LORS DE LA RÉDACTION ET DE LA COMMUNICATION D'UNE DÉCLARATION DE CONFIDENTIALITÉ ?

- Pour chaque catégorie de personnes concernées (par exemple les fournisseurs, clients, travailleurs, visiteurs d'un site Internet, ...) *définissez l'endroit* où la déclaration de confidentialité relative aux traitements qui les concernent sera disponible (par exemple au verso des devis, dans le contrat de travail, sur le site Internet).
- Au besoin (par exemple pour les visiteurs du site Internet, les utilisateurs d'un produit en ligne, les visiteurs d'événements, ...), prévoyez une déclaration de confidentialité sur votre *site Internet* qui informe des traitements de données à caractère personnel pertinents de votre entreprise pour ces personnes concernées (tant en ligne que hors ligne). Prévoyez ensuite un *lien* vers la déclaration de confidentialité sur la page d'accueil ainsi que sur chaque autre page du site Internet afin qu'elle puisse être retrouvée facilement.
- Prévoyez une *traduction* de la déclaration de confidentialité dans toutes les langues du site Internet.
- Apposez une *affiche* de la déclaration de confidentialité dans un lieu accessible au public pour les personnes concernées (par exemple les visiteurs d'un magasin).
- Adaptez le niveau de langue de la déclaration au public :
  - n'utilisez pas de verbes à la voix passive ;
  - évitez les termes complexes et les phrases trop longues ;
  - utilisez un texte « en plusieurs couches » de détail et de complexité (par exemple avec un résumé, des hyperliens qui renvoient vers une version plus détaillée au besoin, ...) ;
  - si vous traitez des données à caractère personnel obtenues auprès d'enfants, la déclaration de confidentialité doit être compréhensible et adaptée à l'âge de l'enfant.
- Datez la déclaration de confidentialité et mettez-la à jour régulièrement en fonction des (changements dans les) traitements. Conservez ces différentes versions.
- Utilisez notre check-list ci-dessous pour ne pas oublier des mentions obligatoires.

QUAND DEVEZ-VOUS COMMUNIQUER UNE « DÉCLARATION DE CONFIDENTIALITÉ » ?

Lorsque vous obtenez les données **directement** auprès de la personne concernée, vous devez communiquer ces informations **au préalable**, et au plus tard **lorsque vous collectez les données à caractère personnel**.

Si vous n'obtenez **pas** les données **directement** auprès de la personne concernée, vous devez communiquer la déclaration de confidentialité :

- au plus tard *dans un délai d'un mois* à compter de l'obtention des données à caractère personnel ;
- si vous recevez ces données à caractère personnel afin de contacter la personne concernée, *au moment de ce premier contact* ; ou
- si vous souhaitez partager ces données à caractère personnel avec une autre entreprise, au plus tard lors du *premier partage* de ces données.

QUE DEVEZ-VOUS COMMUNIQUER POUR ÊTRE SUFFISAMMENT TRANSPARENT ?

Si, en tant que responsable du traitement, vous **recevez** des données à caractère personnel au sujet d'une **personne concernée**, vous devez au moins communiquer à cette personne concernée les informations de la check-list ci-dessous pour (l'ensemble des) traitements de données à caractère personnel. Il peut en outre être nécessaire de donner également des informations au sujet des risques.

Check-list pour la déclaration de confidentialité en cas d'obtention directe auprès des personnes concernées :
Vous pouvez cochez les cases lorsque les éléments ont été ajoutés à votre déclaration de confidentialité.

- ☐ l'identité et les coordonnées (par exemple le nom, l'adresse, ...) du responsable du traitement (ou de son représentant si c'est à l'étranger) ;
- ☐ les coordonnées (par exemple une adresse e-mail DPO) du délégué à la protection des données (**DPO**), si ce dernier a été désigné ;
- ☐ les *finalités du traitement* et le *fondement* précis *du traitement* (par exemple le consentement, la nécessité pour l'exécution du contrat, l'intérêt légitime, ...), et *si* ce fondement du traitement est l'intérêt légitime, une (brève) *précision de cet intérêt* ;
- ☐ lorsque les données à caractère personnel sont transférées, les *destinataires ou catégories de destinataires* des données à caractère personnel (par exemple un développeur de sites Internet, le secrétariat social, ...) ;
- ☐ si les données à caractère personnel sont (seront) transmises en dehors de l'Espace économique européen : l'existence ou non d'une *décision d'adéquation* ou les *garanties qui sont prévues* (par exemple un contrat « qui offre un niveau de protection adéquat », comme par exemple les clauses contractuelles types, ...) et à quel endroit on peut les consulter ou en obtenir une copie ;
- ☐ le *délai de conservation* des données à caractère personnel, ou s'il n'est pas défini, les *critères* qui déterminent ce délai de conservation (par exemple des délais imposés par la législation comptable, ...) ;
- ☐ les *droits* précis de la personne concernée ;
- ☐ le fait que la personne concernée a le droit de *retirer* son consentement à tout moment;
- ☐ le fait que la personne concernée a le droit *d'introduire une réclamation* auprès d'une autorité de contrôle ;
- ☐ le fait de savoir si la fourniture de données à caractère personnel est une *obligation* légale ou contractuelle ou si elle est *nécessaire*, et si la personne concernée est

tenue de fournir les données à caractère personnel et quelles sont les éventuelles *conséquences* de la non-fourniture de ces données ;

- ☐ l'existence d'une *prise de décision automatisée* et les informations utiles concernant la logique sous-jacente ainsi que *l'importance et les conséquences* de ce traitement pour la personne concernée.

- ☐ les (catégories de) données et la source (publique) d'où proviennent les données à caractère personnel, si vous n'avez pas obtenu les données à caractère personnel directement auprès de la personne concernée.

7. QUE DOIS-JE FAIRE SI UNE PERSONNE CONCERNÉE DEMANDE COMMENT JE TRAITE SES DONNÉES À CARACTÈRE PERSONNEL ?

Les entreprises qui sont un responsable du traitement doivent informer les personnes concernées de leurs droits issus du RGPD, dont le droit d'accès. Ce droit d'accès signifie qu'une personne concernée peut demander à une entreprise (i) *si* cette entreprise collecte ou utilise des données à caractère personnel de cette personne concernée et (ii) *lesquelles*. Si tel est le cas, cette entreprise doit communiquer *quelles* données à caractère personnel de cette personne concernée sont traitées et donner accès à celles-ci, plus précisément en transmettant une *copie* de ses données à caractère personnel, gratuitement et avec les explications requises. La transmission d'une copie se fait sous une forme électronique d'usage courant si la personne concernée a introduit une demande de consultation par voie électronique (par exemple par e-mail), sauf si elle demande qu'il en soit autrement (article 15 du RGPD). Vous trouverez plus d'informations sur ce droit d'accès ici.

COMMENT RÉPONDRE À UNE DEMANDE D'ACCÈS ?

Vous devez répondre à la personne concernée le plus rapidement possible et au plus tard **dans un délai d'un mois à compter de la réception de la demande d'accès**. Au besoin, ce délai peut être prolongé de deux mois si la demande est complexe ou en cas de nombreuses demandes. Une telle prolongation doit également être communiquée dans un délai d'un mois.

Vous devez fournir ces informations **gratuitement**.

Si vous faites appel à un **sous-traitant**, il est recommandé de convenir qu'il vous transfèrera d'office de telles demandes dans un délai déterminé (par exemple 5 jours ouvrables), du fait que vous êtes le responsable du traitement.

Base légale : Articles 12 et 15 du RGPD

8. LE CONSENTEMENT DE LA PERSONNE CONCERNÉE EST-IL LA SEULE BASE ME PERMETTANT DE TRAITER DES DONNÉES À CARACTÈRE PERSONNEL ?

Le traitement de données à caractère personnel est permis s'il existe à cet effet un fondement légal. Toutefois, en plus du consentement libre, spécifique et informé, il existe différents autres fondements de traitement.

La demande de consentement ne constitue en d'autres termes qu'un des fondements possibles et n'est requis que lorsqu'une entreprise ne peut se baser sur aucun autre fondement légal.

Si vous pouvez vous baser sur un autre fondement que le consentement, il est préférable de ne pas demander ce consentement, car il peut toujours être retiré (article 7.3 du RGPD).

COMMENT RECUEILLIR VALABLEMENT LE CONSENTEMENT ?

Pour pouvoir parler d'un consentement valable, ce dernier doit être :

- donné librement ;
- spécifique ;
- informé ; et
- indubitable.

Attention : Lorsqu'une personne concernée (par exemple un travailleur) n'a *pas d'autre choix* que de consentir, le consentement n'est pas considéré comme étant libre et n'est généralement pas valable. La personne concernée doit aussi recevoir *au préalable* une bonne description de la finalité du traitement afin qu'elle puisse faire un choix éclairé quant au fait de donner ou non son consentement. Par ailleurs, dans certains cas, le consentement doit également être donné par un *acte positif clair* (les cases cochées d'avance ne sont pas permises) ou une déclaration (Article 4(11) RGPD). Tant que le traitement est en cours, le responsable du traitement doit pouvoir démontrer qu'un consentement valable a été obtenu.

Attention : Le consentement doit également être demandé *de manière visiblement distincte et donc être séparé* du consentement qui est éventuellement demandé pour d'autres choses (par exemple l'acceptation des conditions générales) : cela peut se faire en plaçant par exemple le consentement dans un cadre distinctif sous ces conditions générales ou sur un écran distinct. Le consentement au traitement de données *ne peut pas non plus être lié* au consentement pour l'exécution d'un contrat (par exemple le consentement pour le téléchargement d'une application, ...) et doit donc être demandé séparément.

Base légale : Articles 4(11) et 7 du RGPD

Pour plus d'informations, voir les lignes directrices 5/2020 relative au consentement du Comité européen de la protection des données (EDPB).

DÉCISION DE LA CHAMBRE CONTENTIEUSE AU SUJET D'UNE PLATEFORME DE RÉSEAU SOCIAL ET DU CONSENTEMENT

La Chambre Contentieuse a infligé une amende de 50.000 euros à un réseau social de portée internationale pour la récolte et l'utilisation de données à caractère personnel dans le cadre d'une fonction «inviter des contacts». Avec cette fonction, les membres-utilisateurs du réseau social pouvaient inviter des contacts sur la plateforme (indépendamment du fait qu'ils soient déjà membres-utilisateurs ou non). D'une part, le réseau social collectait et conservait des données relatives à des contacts et d'autre part, il envoyait des invitations à des personnes qui avaient été ajoutées par l'utilisateur.

La Chambre Contentieuse a retenu, entre autres, les violations suivantes du RGPD :

- **Absence de consentement** des personnes concernées qui ne sont pas membre-utilisateur du réseau : le consentement du membre-utilisateur ne suffit pas pour traiter des données de non-membres. Le réseau traitait donc des données personnelles sans base légale valable (infraction à l'article 6 du RGPD) ;

- Le consentement du membre-utilisateur du réseau qui souhaitait inviter ses contacts n'était **donc pas valable puisqu'il était confronté à des options pré-cochées lors du processus d'ajout de contacts** (infraction aux articles 4(11) et 7 du RGPD). Cette pratique est contraire aux conditions du consentement au sens du RGPD, celui-ci doit notamment être libre et constituer un acte positif et univoque : la personne doit donc elle-même cocher les cases souhaitées.

Vous trouverez ici l'intégralité de la décision du 14 mai 2020 de la Chambre Contentieuse.

9. LES PME DOIVENT-ELLES TENIR UN REGISTRE DES ACTIVITÉS DE TRAITEMENT ?

Toute entreprise qui traite des données à caractère personnel (sauf exception reprise ci-dessous) doit en principe tenir un registre des activités de traitement pour toutes les activités de traitement qui relèvent de sa responsabilité. Ce registre est une sorte d'inventaire de tous les traitements et est utile pour évaluer correctement les obligations du RGPD et les risques éventuels.

Vous trouverez ici un exemple de registre des activités de traitement sous la forme d'un fichier électronique à compléter, publié par l'Autorité française de protection des données (CNIL), que vous pouvez utiliser pour le registre de votre entreprise.

À noter que pour les entreprises qui emploient *moins de 250 personnes,* un registre n'est toutefois *pas* requis. La portée de cette exception est toutefois limitée, étant donné qu'elle ne s'applique pas s'il est question de traitements à risques, de traitements de données sensibles ou de traitements intégrés dans le fonctionnement quotidien de l'entreprise comme la gestion du personnel, des clients et des fournisseurs. Si vous avez des doutes sur le fait que cette exception s'applique à votre entreprise, nous vous conseillons de tenir quand même un tel registre, certes de manière simple.

Toute entreprise doit évaluer régulièrement tous les traitements et au besoin, compléter ou adapter le registre.

Base légale : Article 30 du RGPD

Exemple 1 : Une PME comptant cinq membres du personnel gère une plateforme pour le partage de radiographies de patients et d'autres données. Il s'agit de « données sensibles ». Un registre est requis.

Exemple 2 : Une entreprise unipersonnelle de marketing « vend » des données d'e-mails ainsi que des données de profil (de clics) à des tiers La collecte, l'enregistrement et la communication à des tiers de ces données à caractère personnel n'est pas une activité accessoire mais principale. Un registre est requis.

10. QUE PEUT-ON FAIRE SI UN SOUS-TRAITANT NE VEUT PAS SIGNER DE CONTRAT DE SOUS-TRAITANCE ?

La signature d'un contrat de sous-traitance entre le responsable du traitement et le(s) sous-traitant(s) est toujours obligatoire.

Base légale : Article 28.3 du RGPD

Vous trouverez ci-dessous quelques conseils pour l'imposer :

- Vous pouvez utiliser comme fil conducteur le modèle de contrat de sous-traitance publié par l'Autorité danoise de protection des données (disponible également en français et en néerlandais) ;
- Vous pouvez signaler que la signature d'un contrat de sous-traitance est une obligation légale pour les deux parties et que l'APD intervient à l'encontre de responsables du traitement qui ne concluent pas de contrat de sous-traitance (voir la décision cidessous) ;
- Vous spécifiez par exemple dans le contrat principal avec le fournisseur IT que le contrat de sous-traitance fait partie intégrante du contrat entre les parties et, en tant que responsable du traitement, vous joignez votre proposition de contrat en annexe au contrat principal à signer ;
- Vous spécifiez dans le contrat principal que la signature d'un contrat de sous-traitance distinct est obligatoire et que le paiement des prestations peut être suspendu jusqu'à la signature du contrat de sous-traitance.

DÉCISION DE LA CHAMBRE CONTENTIEUSE AU SUJET DE L'OBLIGATION DE CONCLURE UN CONTRAT DE SOUS-TRAITANCE

Le responsable du traitement avait signalé une fuite de données à l'APD, qui avait eu lieu dans le contexte d'un traitement de données à caractère personnel par un sous-traitant établi en Inde. La fuite avait eu lieu après un traitement par le sous-traitant qui n'était pas autorisé par le responsable du traitement et qui était explicitement interdit dans le contrat de sous-traitance conclu entre les parties.

La Chambre Contentieuse a souligné que le responsable du traitement devait prendre *de manière proactive* des mesures techniques et organisationnelles afin de garantir un niveau de protection adéquat (articles 5.1 f), et 24.1 du RGPD) et que le responsable du traitement devait pouvoir démontrer de manière transparente que des mesures avaient été prises (principe de responsabilité repris à l'article 5.2 du RGPD).

La Chambre Contentieuse a fait remarquer à quel point il était important que le responsable du traitement soit rigoureux dans la formulation et le suivi d'un tel contrat de sous-traitance et le respect de toutes les obligations légales à cet égard (comme indiqué à l'article 28.3 du RGPD). Elle considère cela comme une **obligation de résultat**.

Vous trouverez ici l'intégralité de la décision du 8 mai 2020 de la Chambre Contentieuse.

11. QU'EST-CE QU'UNE ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES (AIPD) ET QUAND EST-ELLE OBLIGATOIRE ?

Les différents niveaux de protection que le RGPD veut offrir sont basés sur une analyse de risques. Cela signifie que les entreprises qui sont un responsable du traitement sont obligées, dans certains cas, de réaliser une analyse de risques formelle, à savoir une AIPD.

En général, les entreprises doivent réaliser cette AIPD lorsque la collecte et/ou l'utilisation de données à caractère personnel *est susceptible d'engendrer un risque élevé pour les droits et libertés* des personnes concernées, comme par exemple le droit à la liberté d'expression, à la vie privée, … L'utilisation de données à caractère personnel *implique en particulier un risque élevé* i) en cas de *prise de décision* automatisée au sujet des personnes concernées sur la base d'une évaluation systématique et élargie d'aspects personnels des personnes concernées, ayant des conséquences juridiques qui les affectent (par exemple en cas d'établissement de profils), ii) en cas de collecte et d'utilisation de données à caractère personnel sensibles à *grande échelle* (par exemple des données médicales), et iii) en cas de *surveillance* systématique à grande échelle d'une zone accessible au public (par exemple via une surveillance par caméras).

Vous trouverez ici un logiciel publié par l'Autorité française de protection des données (CNIL) que vous pouvez utiliser pour exécuter une AIPD pour votre entreprise.

Base légale : Article 35 du RGPD. Vous trouverez également plus d'informations ici.

Exemple 1 : Des données à caractère personnel sont collectées auprès de tiers pour ensuite être prises en considération afin de décider de refuser ou de mettre fin à un certain contrat de service avec une personne physique (par exemple une compagnie d'assurances qui consulte une banque de données RSR ou une « liste noire » avant de faire une proposition d'assurance définitive au consommateur). L'entreprise/la PME doit réaliser une AIPD.

Exemple 2 : Des données de santé de patients sont collectées de manière automatisée à l'aide de dispositifs médicaux implantables actifs (par exemple pour la mesure et l'adaptation du taux de glycémie via la puce) qui sont utilisés à grande échelle. L'entreprise/la PME doit réaliser une AIPD.

Exemple 3 : Lorsqu'un traitement de données à grande échelle, généré par exemple via des montres connectées ou des appareils dotés de capteurs qui envoient des données par Internet ou par un autre moyen (application de l'Internet des objets), est utilisé pour une analyse de comportement ou un profilage (par exemple une smartTV qui analyse les préférences et fait des propositions de programmes tv), l'entreprise doit réaliser une AIPD.

Exemple 4 : Une PME qui utilise une plateforme de recrutement en ligne qui sélectionne et rejette automatiquement des candidats sur la base d'une lecture automatique du C.V. doit effectuer une AIPD.

Exemple 5 : Une PME observe systématiquement les habitudes de navigation de membres du personnel afin de prévenir un usage privé excessif pendant les heures de travail. Les travailleurs se trouvent dans une position subalterne et le risque est élevé. L'entreprise doit dès lors réaliser une AIPD.

QU'ENTEND-ON PAR « DONNÉES À CARACTÈRE PERSONNEL SENSIBLES » ?

Les données à caractère personnel « sensibles » sont :

- **des données à caractère personnel qui révèlent :**
  - l'origine raciale ou ethnique ;
  - les opinions politiques ;
  - les convictions religieuses ou philosophiques ;
  - l'appartenance syndicale ;
- **les traitements de données génétiques ;**
- **les traitements de données biométriques en vue de l'identification unique d'une personne ;**
- **les données relatives à la santé ;**
- **les données relatives à la vie sexuelle ou à l'orientation sexuelle.**

Le **traitement** de ces données est **en principe interdit**, sauf si des conditions spécifiques sont respectées.

Base légale : Article 9 du RGPD

Exemple : des fiches médicales, des données de localisation indiquant que tel jour de la semaine, une personne se stationne devant une église ou une mosquée pendant deux heures, un certificat médical, ...

QU'ENTEND-ON PAR DONNÉES ANONYMES ?

Des données anonymes sont des données ne permettant plus d'identifier un individu ou de le rendre identifiable. Dans ce cas, le **RGPD et la Loi relative à la protection des données de 2018 ne sont pas d'application**. Toutefois, grâce aux progrès technologiques, de nombreuses données qui semblent anonymes constituent quand même des données à caractère personnel car elles permettent bel et bien d'identifier des personnes physiques en les combinant à d'autres données à caractère personnel.

La **pseudonymisation** ou le **cryptage** de données à caractère personnel sont des mesures de sécurité qui rendent la lecture de données à caractère personnel, ou leur mise en relation avec des personnes, plus difficile pour des personnes non habilitées (par exemple des hackers). Dans ce cas, le **RGPD et la Loi relative à la protection des données de 2018 restent bien d'application**..

Base légale : Considérant 26 du RGPD

Pour plus d'informations, voir l'avis 05/2014 du Groupe de travail "Article 29" concernant l'anonymisation de données.

12. MON ENTREPRISE DOIT-ELLE DÉSIGNER UN DÉLÉGUÉ À LA PROTECTION DES DONNÉES (DATA PROTECTION OFFICER OU DPO) ?

Une entreprise, aussi bien un responsable du traitement qu'un sous-traitant, doit *obligatoirement* désigner un DPO si ses tâches consistent *principalement* à surveiller de manière régulière et systématique et à grande échelle des personnes concernées et/ou à traiter des données à caractère personnel « sensibles » à grande échelle. Dans tous les autres cas, *il reste conseillé de désigner un DPO, mais ce n'est pas obligatoire.*

Qui peut assurer le rôle de DPO ? Un travailleur existant ayant des connaissances suffisantes du RGPD (si les tâches professionnelles du collaborateur sont compatibles avec celles du DPO et si cela ne donne pas lieu à des conflits d'intérêts) ou une personne externe. Le DPO doit donc pouvoir effectuer ses tâches de manière indépendante et doit pouvoir faire rapport directement au niveau le plus élevé de la direction.

Soyez donc très attentifs aux cas où la désignation d'un DPO est obligatoire (article 37.1 du RGPD) et veillez, le cas échéant, à ce que cette personne puisse exercer sa fonction en toute indépendance et en connaissance de cause (article 38 du RGPD).

Exemple : L'administrateur d'une société ne peut pas être le DPO de cette société, étant donné que le DPO doit être indépendant. Cet administrateur ne peut pas être indépendant du fait qu'il poursuit les intérêts de la société.

Base légale : Articles 37 et suivants du RGPD

Pour plus d'informations, voir les lignes directrices concernant les délégués à la protection des données du Groupe de travail « Article 29 » ainsi que le dossier thématique de l'APD.

DÉCISION DE LA CHAMBRE CONTENTIEUSE AU SUJET DE LA FONCTION DU DPO

La Chambre Contentieuse a infligé une amende de 50.000 euros pour non-respect de l'obligation relative à la fonction de DPO.

En vertu de l'article 38.6 du RGPD, le DPO peut exercer d'autres missions et tâches mais à condition que ces dernières n'entraînent **pas de conflit d'intérêts**. La Chambre Contentieuse a constaté qu'une entreprise n'avait pas respecté cette obligation puisque le rôle du DPO était exercé par le « *Head of the Compliance, Risk Management and Audit department* ». La Chambre Contentieuse a retenu, entre autres, que la combinaison de ces deux rôles entravait l'indépendance de la surveillance effectuée par le DPO sur les opérations de traitements de données personnelles réalisées par le département « *Compliance, Risk Management and Audit* ».

Vous trouverez ici l'intégralité de la décision du 28 avril 2020 de la Chambre Contentieuse.

13. COMMENT PUIS-JE RESTER INFORMÉ(E) DES ÉVOLUTIONS DU RGPD ?

Vous pouvez rester informé(e) des évolutions au niveau national (ainsi qu'au niveau européen) en consultant régulièrement le site Internet de l'APD et en y effectuant des recherches par motsclés et en vous abonnant à la newsletter bimestrielle de l'APD pour les PME dans le cadre du projet BOOST.

14. QUELLES SONT LES SANCTIONS SI MON ENTREPRISE NE RESPECTE PAS OU VIOLE LE RGPD ?

Lorsque votre entreprise ne respecte pas le RGPD, l'APD peut entre autres vous infliger une amende administrative, mais aussi limiter ou interdire des traitements. Votre entreprise peut en outre être condamnée par un tribunal à cesser des pratiques illicites et à payer des dommages-intérêts. Des sanctions pénales peuvent également être infligées.

Base légale : Article 83 du RGPD et Articles 209 et suivants de la Loi relative à la protection des données de 2018.

Vous trouverez plus d'informations dans notre brochure RGPD : Vade-mecum pour les PME, p. 30.

15. QUELLES OBLIGATIONS DOIS-JE RESPECTER SI J'UTILISE DES COOKIES ?

Les Cookies sont de « mini fichiers » placés (par exemple lors du développement d'une application ou d'un site Internet) sur l'appareil d'un utilisateur qui est connecté à Internet, comme un ordinateur, un téléphone, une tablette ou une smartTV. Les Cookies collectent souvent des données à caractère personnel. Dès lors, le RGPD s'applique, entre autres réglementations.

Faites également attention au placement de plug-ins de médias sociaux sur votre site Internet, comme par exemple un bouton « like » de Facebook. La CJUE a précisé dans son arrêt *Fashion ID* qu'une entreprise qui a placé un tel bouton « like » sur son site Internet était conjointement responsable avec le fournisseur de média social.

Vous trouverez plus d'informations sur l'obligation d'information et encore d'autres obligations en cas d'utilisation de cookies sur cette page Internet de l'APD.