**CHECKLIST RGPD pour les professions economiques**

Dès le 25 mai 2018 votre cabinet devra être conforme aux [règles du RGPD](https://www.privacycommission.be/fr/reglement-general-sur-la-protection-des-donnees-0).

Pour ce faire, il s’impose de procéder de manière structurée. La présente checklist a pour objectif de vous aider dans cet exercice.

Les réponses aux différentes questions posées ci-dessous vous permettrons de déterminer où vous vous trouvez dans la mise en conformité au RGPD et de planifier les éventuelles mesures complémentaires à prendre.

Lorsque vous parcourez cette liste, gardez toujours à l’esprit que ce qui est visé concerne la collecte/le traitement/la conservation de **données à caractère personnel[[1]](#footnote-1)** de **personnes physiques** dans le cadre de l’exercice de votre profession.   
Le RGPD parle de « personne concernée » pour désigner la personne physique dont les données à caractère personnel sont traitées.

**12 ETAPES,**

**AUTANT DE BALISES DE REFLEXION**

* **Étape 1- Répertoriez les données personnelles dont vous disposez, leur** **provenance et modalités de conservation.**
* **Etape 2 - Vos traitements de données à caractère personnel sont-ils licites ?**
* **Etape 3 - Attention aux données sensibles !**
* **Etape 4 - Sollicitez-vous le consentement de manière correcte ?**
* **Etape 5 - Garantissez-vous leurs droits aux personnes concernées ?**
* **Etape 6 - Quid de la sécurité de votre système informatique ?**
* **Etape 7 - Devez-vous désigner un DPO ?**
* **Etape 8 - Devez-vous réaliser une DPIA ?**
* **Etape 9 - Comment établir un registre des activités de traitement des données ?**
* **Etape 10 - Mettez en place une politique de protection de la vie privée.**
* **Etape 11- Attention aux relations avec les sous-traitants**
* **Etape 12 – Comment réagir en présence d’une violation de données ?**

# Étape 1 – RéPErtOriez les données personnelles dont vous disposez, leurs provenance et modalités de conservation

Établir une sorte d’ « inventaire des données » est une première étape très importante dans la mise en conformité de votre cabinet au RGPD. Vous devez répertorier toutes les données personnelles[[2]](#footnote-2) que vous traitez[[3]](#footnote-3) dans le cadre de vos activités professionnelles.

Il est recommandé de réaliser cet exercice, par exemple dans un fichier Excel ou toute autre forme de base de données. Ce fichier constituera la base du registre des traitements des données à caractère personnel.

## Quelles sont les personnes dONT VOUS TRAITEZ LES DONNÉES ?

Voici d’ores et déjà diverses catégories de personnes dont les professions du chiffre traitent a priori les données à caractère personnel. Attention : cette liste n’est pas exhaustive. Vous conservez peut-être des données d’autres personnes.

Clients

Fournisseurs

Personnel

Prospects

Autres : par exemple, votre cabinet publie une lettre d’information à l’intention des clients, mais toutes les personnes qui le souhaitent peuvent aussi s’y abonner.

## QUELLES DONNÉES ?

**Quelles catégories de données relatives à des personnes physiques traitez-vous ?**

Données d’identité (nom, adresse, numéro de téléphone, numéro d’entreprise…)

Données de facturation

Données sensibles (santé, photo, affiliation à un syndicat ou à un parti politique, enfants…)

Autres : adresse IP, cookies, plaques d’immatriculation de véhicules…

SOURCE

**Quelle est l’origine de ces données ?**

Les personnes concernées elles-mêmes

Les tiers, par exemple des clients (données relatives à leurs fournisseurs et clients)

Des bases de données publiques telles que la BCE, la Banque Nationale de Belgique…

Des bases de données privées telles que Companyweb, Graydon…

STOCKAGE/ACCÈS/CONSERVATION ?

**Où sont stockées les données personnelles que traite votre cabinet ? Quelles bases de données et à quel endroit ?**

Serveur au cabinet

Serveur chez un prestataire spécialisé

Cloud géré par vous

Cloud chez un prestataire (Google, Microsoft, Proximus…)

Archives – papier

…

**Combien de temps conservez-vous les données ?**

Exemples :

La législation comptable exige que les données soient conservées pendant 7 ans.

Le réviseur d’entreprises qui a exécuté une mission révisorale conserve le dossier d’audit pendant une durée de cinq ans à dater du rapport qui a été établi sur la base du dossier d’audit.

La loi anti-blanchiment prévoit l’obligation que les données collectées dans ce contexte soient conservées pendant 10 ans après la fin de la relation avec le client.

*Attention*: les données à caractère personnel ne peuvent pas être conservées plus longtemps que ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. La durée de la conservation des données à caractère personnel dans le cabinet doit donc faire l’objet d’une réflexion approfondie afin de pouvoir être justifiée le cas échéant.

**Qui dispose d’un accès à ces bases de données ? Quelles sont les fonctions de ces personnes ? Cet accès est-il nécessaire ?**

Etablissez un tableau/organigramme des tâches respectives de chacun et examinez à quelles données à caractère personnel chaque personne doit avoir accès dans le cadre de l’exécution de ses tâches.

**L’accès est-il sécurisé ?**

Prenez les mesures nécessaires afin de limiter l’accès aux données à caractère personnel. Il peut s’agir d’une protection par des moyens numériques (login, mot de passe), mais aussi d’une serrure sur l’armoire dans laquelle des documents sont conservés. Dressez un aperçu des différentes mesures de protection mises en œuvre dans votre cabinet.

[Checklist informatique](https://www.ibr-ire.be/fr/l_institut/actualites/actualites_ire/Documents/2018-03-20-ICTChecklist-NL-FR.xlsx)

[Guide des bonnes pratiques informatiques](https://www.ibr-ire.be/fr/l_institut/actualites/actualites_ire/Documents/guide-des-bonnes-pratiques-informatiques.pdf)

**Ces données à caractère personnel sont-elles partagées ou communiquées à des tiers ? Transférées dans l’Union européenne ou en dehors (cloud) ?**

Les données à caractère personnel sont partagées avec :

* le secrétariat social (personnel du cabinet) ;
* l’administration fiscale (déclarations TVA des clients, listings TVA, fiches fiscales…) ;
* …

# Étape 2 - VOS TRAITEMENTS de donnÉes À caractÈre personnel SONT-IlS LiCITES ?

Vous pouvez collecter et traiter des données à caractère personnel uniquement dans le cadre de l’un des fondements énumérés par l’article 6 du RGPD.

**Pourquoi est-ce aujourd’hui vraiment important de déterminer le fondement licite du traitement ?**

Les droits de la personne concernée peuvent varier selon le fondement retenu. Par exemple, la personne concernée pourra davantage appuyer sa demande de suppression de ses données si celles-ci ont été traitées sur base de son consentement (étape 4).

Le fondement doit également être précisé dans une politique de la vie privée (cf. étape 10) .

**Pourquoi conservez-vous ces données à caractère personnel ?**

exécution d’un contrat ou d’une lettre de mission

gestion du personnel

obligations légales (loi anti-blanchiment, listing TVA…)

gestion des relations avec les clients, les fournisseurs et d’autres tiers

missions judiciaires

sans raison spécifique

autre …

**Examinez les types de traitement de données que vous exécutez et déterminez, au regard du RGPD, leur fondement licite**

Vous traitez des données à caractère personnel :

La personne concernée a donné son consentement ; par exemple, elle s’est abonnée à la lettre d’information électronique du cabinet.

Le traitement est nécessaire à l’exécution d’un contrat ; par exemple si un client transmet des factures à traiter dans la comptabilité, il va de soi que vous pouvez traiter les données à caractère personnel mentionnées sur ces factures. De même, si un client effectue un paiement en ligne, vous pouvez bien entendu traiter les données de la carte de crédit de ce client afin d’obtenir le paiement.

Le traitement est nécessaire au respect d’une **obligation légale** :

Si vous êtes employeur, vous devez transmettre les données de vos salariés à la sécurité sociale (DIMONA).

obligations fiscales : listing TVA, fiches fiscales, IPP

loi anti-blanchiment

autres obligations légales …

Le RGPD prévoit d’autres fondements[[4]](#footnote-4) au traitement des données à caractère personnel, mais ceux-ci seront en principe rarement d’application pour les professions du chiffre.

# Étape 3 - Attention aux donnÉes sensibles !

Le traitement de données sensibles est, en principe, **interdit** (art. 9 RGPD).

Les données sensibles sont les suivantes : origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques ou appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d’identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l’orientation sexuelle.

Néanmoins, l’interdiction de traitement de ces données connaît diverses exceptions, à l’exemple : [[5]](#footnote-5)

❖ En cas de consentement explicite de la personne concernée ;

❖ Afin de satisfaire à une obligation légale ;

❖ En vue de la sauvegarde d’intérêts vitaux.

Concrètement : en tant que professionnel du chiffre, il arrive que vous preniez connaissance de données sensibles. Par exemple, lorsque vous complétez la déclaration IPP d’une personne qui est membre d’un syndicat ou qui siège dans un conseil communal pour un parti politique donné ou lorsque vous complétez la déclaration IPP d’un couple homosexuel. Vous êtes responsable de la comptabilité d’un parti politique local. Vous conservez une copie de cartes d’identité électroniques ou de passeports contenant des données biométriques. Vous tenez la comptabilité d’un médecin et prenez donc connaissance de sa patientèle.

Cochez et complétez si nécessaire, les situations rencontrées dans votre cabinet :

Je traite des données sensibles :

Je relève d’une des exceptions précitées, à savoir :

Obligations légales : loi anti-blanchiment / CIR (déclaration de revenus)

Le traitement de données à caractère personnel relatives aux condamnations pénales et aux infractions n’est également autorisé que dans certaines conditions (art. 10).

Je traite des données à caractère personnel relatives aux condamnations pénales et aux infractions : comptabilité/audit d’un cabinet d’avocats, par exemple.

OUI  / NON

# Étape 4 - SOLLICITEZ-vous le consentement de maniÈre correcte ?

Hormis s’il existe un autre fondement licite (cf. étape 2), le traitement des données à caractère personnel nécessite le consentement de la personne concernée. Tel sera notamment le cas si votre cabinet souhaite collecter des données à caractère personnel pour diffuser une lettre d’information électronique, une invitation à des événements tels que des séminaires, etc.

La demande de consentement est un acte très important dans le RGPD. Selon le RGPD, le consentement doit être **libre, spécifique, éclairé et univoque**. En outre, le consentement doit toujours être un acte positif clair (art. 4, 11° et art. 7). Le fait de précocher une case par défaut sur votre site n’est pas constitutif d’un consentement explicite.

Vérifiez ce qu’il en est dans votre cabinet et complétez si nécessaire :

□ Je prévois pour le consentement un choix libre : la personne concernée peut donner son consentement de manière explicite (« opt-in »).

□ J’explique clairement à la personne concernée à quelles fins elle donne son consentement (cf. droit à l’information).

□ Je ne déduis pas le consentement d’un silence, d’une case cochée par défaut ou d’une absence d’action.

□ Je prévois la possibilité pour la personne concernée de retirer à tout moment son consentement. Retirez son consentement est aussi simple que de le donner ; les modalités de retrait sont clairement indiquées.

Il est également important que le consentement donné puisse toujours être contrôlé. Cela implique que vous devez pouvoir démontrer qui a donné son consentement, quand et comment. Enregistrez de préférence ces informations dans un document, par exemple à l’aide des historiques des connexions au site web ou d’un système de signature électronique.

□ Le consentement est contrôlable.

**Attention : enfants de moins de 16 ans !**

Si, en tant que professionnel du chiffre, vous traitez des données à caractère personnel relatives à des enfants de moins de 16 ans, un parent ou un tuteur doit donner son consentement (art. 8 RGPD). Toutefois, cette obligation ne s’applique que si le traitement repose sur le consentement et s’il s’agit de services de la société de l’information (réseaux sociaux, p. ex.). En règle générale, une telle situation ne se rencontre pas pour les professions du chiffre.

Cette disposition ne porte pas atteinte au droit des obligations belge (p. ex., les règles relatives à la validité, à la formation ou aux effets d’un contrat à l’égard d’un enfant).

En outre, vous devez pouvoir prouver que vous avez entrepris des démarches raisonnables aux fins de vérifier que le consentement a été donné.

Cochez la situation dans votre cabinet :

□ Je conserve des données relatives à des enfants de moins de 16 ans, sur la base d’un consentement.

□ J’utilise un système qui me permet de vérifier le consentement auprès des parents/du tuteur.

**Qu’advient-il du consentement donné dans le passé ?**

Si le consentement donné dans le passé satisfait aux nouvelles exigences, vous ne devez pas demander un nouveau consentement. S’il ne remplit pas les conditions, vous devez demander un nouveau consentement de manière correcte.

****

[MODELE DISPONIBLE : clause de consentement](https://www.ibr-ire.be/fr/l_institut/actualites/actualites_ire/Documents/01-FR-clause-de-consentement.docx)

# EtAPE 5 - GARANTISSEZ-VOUS LEURS DROITS AUX PERSONNES CONCERNEES ?

Dans votre cabinet, vous devez tenir compte de l’ensemble des droits que le RGPD reconnait aux personnes concernées. Dressez un état des lieux et effectuez, le cas échéant, les adaptations.

Il est important est de savoir quelle sera votre réaction si quelqu’un entend exercer ses droits. Qui sera, en l‘occurrence, responsable ? La personne responsable sait-elle comment réagir ? Quid des possibilités techniques ?

Principe : l’exercice des droits des personnes concernées requiert une communication explicite et des règles précises (art. 12 RGPD)

Toute information et communication doit être délivrée d’une part d’une façon concise, transparente, compréhensible et aisément accessible et d’autre part, en des termes clairs et simples.

Vous pouvez ici utilement faire usage d’une **« politique de protection de la vie privée»** qui reprend ces droits et explicite les modalités d’exercice de ces droits.

Ces droits trouvent toujours à s’appliquer, sauf si des dispositions légales prévoient une exception : pour les professions du chiffre, il s’agit de la **loi antiblanchiment**. Il est important de le mentionner explicitement dans votre politique de protection de la vie privée.

! Pour **les données sans rapport avec la loi antiblanchiment** (par exemple, les personnes que vous invitez dans le cadre d’évènements), les règles suivantes sont intégralement d’application : si une personne concernée fait une demande pour exercer ses droits, vous devez réagir dans un délai d’un mois après la réception de la demande. En fonction de la complexité de la demande, ce délai peut être prolongé de deux mois supplémentaires.

Faites le test : les droits ci-dessous sont-ils effectivement accordés dans votre cabinet ? Repérez quand ils ne sont pas d’application.

□ **Droit à l’information** (art. 13 et 14 RGPD)

Je n’effectue aucun traitement de données sans que les personnes concernées en aient eu connaissance ?

Notre politique de la vie privée est mentionnée sur notre site

Notre politique de la vie privée est reprise en annexe de la lettre de mission/ conditions générales

Notre politique de la vie privée est explicitée et mise à disposition dès le premier contact.

Le règlement précise les informations à communiquer à votre client, par exemple via la politique de vie privée. Cette obligation trouve à s’appliquer indépendamment du fait que les données sont collectées directement ou indirectement auprès du client.

□ **Droit d’accès**  (art. 15 RGPD)

La personne dont vous traitez les données a le droit d’y accéder et d’obtenir des informations sur les finalités du traitement. Je prévois également de délivrer une copie des données à caractère personnel traitées dans le mois (prolongation possible de deux mois supplémentaires)

□ **Droit à la rectification (**art. 16 RGPD)

La personne dont vous traitez les données a le droit de corriger celles qui sont inexactes ou incomplètes.

□ **Droit à l’effacement, droit à l’oubli numérique** (art. 17 RGPD)

Dans une série de circonstances spécifiques, la personne dont vous traitez les données a le droit de demander leur effacement et le retrait de votre base de données.

Vous pouvez refuser d’accéder à cette demande d’effacement dans une série de cas précisés à l’article 17 du règlement.

□ **Droit à la limitation du traitement** (art. 18)

Sous certaines conditions énumérées à l’article 18, la personne concernée a le droit de demander la limitation du traitement de ses données personnelles.

□ **Droit à la portabilité des données** (art. 20 RGPD)

Chaque personne dont vous traitez les données personnelles a le droit de demander de les transmettre à une autre entreprise.

Ces données doivent être transmises gratuitement, dans un délai d’un mois, (prolongation possible de deux mois- dans un « format structuré, couramment utilisé et sous une forme lisible de manière électronique »).

Il doit nécessairement s’agir d’un traitement effectué à l’aide de procédés automatisés, fondé sur le consentement de la personne ou sur un contrat.

 pas d’application

□ **Droit d’opposition** (art. 21 RGPD)

Chaque personne dont vous traitez les données a le droit de s’opposer à tout moment, pour des raisons tenant à sa situation particulière, à leur traitement (sauf si obligation par ou en en vertu de la loi ou si c’est nécessaire à l’exécution d’un contrat).

Lorsque les données à caractère personnel sont collectées à des fins de *direct marketing*, la personne concernée peut s'opposer, gratuitement et sans aucune justification, au traitement envisagé des données à caractère personnel la concernant.

□ **Décision individuelle automatisée,** y compris le profilage(art. 22 RGPD)

Chaque personne dont vous traitez les données a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé,

Ce droit ne s'applique pas lorsque la décision est prise 1) dans le cadre d'un contrat ; 2) est fondée sur une disposition prévue par ou en vertu d'une loi ; 3) est fondée sur le consentement explicite de la personne concernée.

# ETAPE 6 - QUID de La SECURITE DE VOTRE SYSTEME INFORMATIQUE ?

Le RGPD vous oblige en ordre principal à assurer la sécurité de votre propre base de données. Faites usage de cette [checklist](https://www.ibr-ire.be/fr/l_institut/actualites/actualites_ire/Documents/2018-03-20-ICTChecklist-NL-FR.xlsx) et utilisez comme cadre de référence la norme ISO 27001 ‘Management de la sécurité de l’information », disponible sur [**l’Iso Store**](https://www.iso.org/fr/standard/64120.html)

* Quelles sont les procédures utilisées pour se logger ?
* Tous les softwares sont-ils accessibles à tout le monde ? Existe-il une gestion des mots de passe ?
* Quelles sont les modalités de mises à jour dans votre système : antivirus/firewall/windows ou Ios ?
* La politique de backup prévoit-elle qu’une sauvegarde intégrale du système doit être effectuée au moins tous les huit jours ?

Les collaborateurs sont-ils au courant des modalités de gestion des mots de passe et des règles de base relatives aux mesures de sécurité (par exemple, ne jamais laisser un appareil en accès libre) ?

# ETAPE 7- DEVEZ-Vous DESIGNER un Data Protection Officer (DPO) ?

La désignation d’un DPO (Délégué à la Protection des Données) est une nouveauté importante. Il s’agit d’une personne qui, sur la base de ses connaissances spécialisées et de ses pratiques en matière de protection des données, est susceptible d’assister l’entreprise dans le cadre de l’examen de sa conformité aux règles du RGPD (art. 37-39 du RGPD)

**Quand faut-il désigner un DPO ?**

Une telle obligation **ne s’applique pas a priori** aux professions du chiffre. Même si vous n’êtes pas obligé de désigner un DPO, il peut toutefois s’avérer utile de prévoir une personne au sein de votre cabinet en charge de s’occuper des différents aspects liés à la protection de la vie privée, sans pour autant qu’elle soit explicitement désignée comme DPO.

Le RGPD rend la désignation d’un DPO obligatoire au sein des entreprises dans les deux hypothèses suivantes :

□ Vous êtes principalement en charge du traitement des données sensibles (cfr. Étape 2)?

□ Vous êtes principalement en charge du traitement des données personnelles qui requiert régulièrement et systématiquement des observations à grande échelle ?

A l’évidence, ce dernier cas est très vague. Il convient de l’interpréter dans le sens où le traitement des données personnelles constitue votre *core business*. Par exemple, parce que le direct marketing ou le profilage font partie intégrante de votre business. En outre, ce type d’activité doit concerner une quantité considérable de données personnelles.

# ETAPE 8 -DEVEZ-VOUS REALISER UNE Data Protection Impact Assessment (DPIA) ?

L’application du RGPD impose à certaines entreprises de (faire) réaliser une AIPD (analyse d’impact préalable relative à la protection des données) une forme d’audit de sécurité dans le cadre de traitements définis.

Une telle analyse n’est, en principe, pas requise pour les professions du chiffre.

Vous trouverez davantage d’information sur la AIPD sur le site de la Commission vie privée ainsi que dans les directives du groupe de travail 29[[6]](#footnote-6). Dans l’hypothèse ou une DPIA devrait être réalisée, nous vous conseillons pour son déroulement de recourir à un expert.

# ETAPE 9 - ETABLIR UN REGISTRE DE VOS ACTIVITES DE TRAITEMENT

Chaque cabinet qui traite des données personnelles va devoir établir un registre de ses activités de traitement et le tenir à jour (art. 30 RGPD).

Ce registre devra au moins contenir les données suivantes :

□ nom et coordonnées du responsable du traitement et le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données (DPO)

□ Finalités du traitement [voir étape 1] ;

□ Description des catégories concernées et des données personnelles corrélatives [voir étape 2] ;

□ Les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées (en autres, les destinataires dans les pays tiers ou les organisations internationales [voir étape 1) ;

□ Dans la mesure du possible, les délais prévus pour l’effacement des différentes catégories de données [voir étape 1] ;

□ Dans la mesure du possible, une description générale des mesures techniques et organisationnelles de sécurité [voir étape 6]

Si d’application, transfert des données personnelles à un pays tiers ou une organisation internationale, en ce compris la mention de ce pays tiers ou de cette organisation internationale, et si nécessaire des documents relatifs aux garanties appropriées.

La Commission vie privée propose sur son site un [modèle de registre des activités de traitement](https://www.privacycommission.be/fr/canevas-de-registre-des-activites-de-traitement) susceptible d’aider les entreprises et organismes à établir un tel registre. Ce modèle n’est pas un support officiel, vous êtes libre d’utiliser un autre registre qui peut se présenter **sous un autre format (autre logiciel, … ), pour autant que son objectif soit maintenu : fournir un aperçu complet des traitements opérés de données à caractère personnel.**

**Ce document est particulièrement important, car il forme la base sur laquelle l’Autorité de protection des données (anciennement la Commission de la vie privée) s’appuiera dans le cadre d’un éventuel contrôle (par exemple, suite à une plainte ou un violation de données) pour établir si le cabinet répond aux exigences de conformité du RGPD).**

# ETAPE 10 - METTez EN PLACE une POLITIQUE DE PROTECTION DE LA VIE PRIVEE (art. 24.2)

Cet exercice est une excellente opportunité pour établir une politique de protection de la vie privée ou évaluer la politique existante (par ex, selon la norme ISQC1) et y intégrer les obligations du RGPD.

Ce document doit au moins comporter les éléments suivants :

vos coordonnées en tant que responsable du traitement des données – données DPO ou de la personne responsable de la protection des données au sein du cabinet - [voir étape 7]

L’identité de l’éventuel sous-traitant et les modalités de traitement des données à caractère personnel [voir étape 11]

□ La base légale des traitements de données [voir étape 1]

□ La durée de conservation des données [voir étape 1]

□ Le cas échéant, les informations relatives aux transferts de données hors de l’UE [voir étape …]

□ La possibilité pour la personne concernée d’introduire une plainte auprès de l’Autorité de protection des données (anciennement la Commission Vie privée) si elle constate que ses données personnelles sont erronées dans leur traitement [voir étape ..]

□ Les droits des personnes concernées [voir étape 5] ;

□ Les mesures techniques et organisationnelles que vous prendrez pour être conforme au RGPD

□ Les finalités du traitement des données [voir étape 1] ;

Il est important d’être transparent (voyez droit à l’information – art. 13 et 14 du RGPD) en mettant ce texte à disposition sur votre site. En tout état de cause dans le cadre de la protection de la vie privée, il doit autant que possible être fait usage d’un langage clair et compréhensible sur le fond.

****[MODELE : politique de protection de la vie privée](https://www.ibr-ire.be/fr/l_institut/actualites/actualites_ire/Documents/02-FR-politique-de-confidentialite.docx)

# ETAPE 11 - relatiONS AVEC LES SOUS-TRAITANTS (art. 28)

Il vous est loisible de désigner un sous-traitant pour assurer le traitement des données personnelles. En votre qualité de responsable du traitement des données, vous devez vous assurer de la conformité RGPD des contrats avec les travailleurs (contactez votre secrétariat social) ainsi que des sous-traitants.

Dans le cadre du nouveau règlement, vous devez également pouvoir garantir que vous n’avez des relations professionnelles qu’avec des entreprises sécurisées. Dans l’hypothèse où vous sous traitez certaines activités, il est important de juger si les mesures de sécurité initialement prévues ans les contrats existants sont efficientes et suffisantes au regard des obligations du RGPD.

Effectuez une évaluation des contrats existants avec les fournisseurs et sous-traitants et agissez en temps utile pour effectuer les adaptations nécessaires

□ je suis attentif à toujours disposer de contrats écrits présentant les garanties requises en matière de sécurité.

# Etape 12 - COMMENT REAGIR EN PRéSENCE d’UNE VIOLATION DE DONNEES ?

Si vous êtes confronté à une violation de données, (par ex, votre système est hacké et vos données sont volées), vous êtes tenu de respecter un devoir de communication (promptement ou endéans, en tout cas, les 72 heures) qui suivent le moment du constat.

• a) Obligation de notification à la Commission vie privée (art. 33 RGPD)

En cas de violation de données à caractère personnel, vous devez notifier cette violation a la Commission Vie privée, dans les 72 heures après en avoir pris connaissance si la violation en question est susceptible de générer un risque pour les droits et libertés des personnes physiques. Par exemple, une violation du secret professionnel.

• b) Communication à la personne concernée (art. 34 RGPD)

Lorsque la violation de ses données personnelles est susceptible de présenter un risque élevé pour les droits et libertés de la personne concernée, il est indubitable qu’il doit en être averti dans les meilleurs délais. Par exemple, en cas de vol de données bancaires non cryptées.

L’obligation de communication à la personne concernée ne trouve pas à s’appliquer dans les cas suivants :

* Vous avez déjà mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite violation (par ex . cryptage) ;
* Vous avez pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées n’est plus susceptible de se matérialiser;
* La communication exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace)

La notification à la Commission vie privée et la communication a la personne concernée doit comporter une série de données (voyez la page spécifique sur le site de [la Commission vie privée](https://www.privacycommission.be/fr/la-notification-de-fuites-de-donn%C3%A9es)). Vous êtes également obligé d’établir un récapitulatif détaillé de toutes les violations produites.

Application concrète dans votre cabinet ?

□ Désignez une personne responsable du contrôle et de la notification / communication des violations …………………………………………………………………………………………………………………………………………….

□ Préparez un document pour la notification/communication des violations.

Essayez d’établir préalablement une évaluation du risque pour les droits et les libertés des personnes dans l’hypothèse ou – de quelque manière que ce soit – ces données personnelles seraient perdues. Indépendamment de cette estimation, préparez-vous le mieux possible pour réagir dans le cadre d’une violation de données. Nous vous conseillons de prendre contact avec votre responsable/fournisseur IT.

1. Données à caractère personnel : toute information se rapportant à une **personne physique** identifiée ou identifiable ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu’un nom, un numéro d’identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. [↑](#footnote-ref-1)
2. Données à caractère personnel = toute information se rapportant à une **personne physique** identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement,

   notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale; [↑](#footnote-ref-2)
3. Traiter = collecter, enregistrer, organiser, conserver, adapter, modifier, extraire, consulter, utiliser, communiquer par transmission, diffuser ou toute autre forme de mise à disposition, rapprocher ou interconnecter, limiter, effacer ou détruire des données à caractère personnel. [↑](#footnote-ref-3)
4. le traitement est **nécessaire à la sauvegarde des intérêts vitaux** de la personne concernée ou d’une autre personne physique ;

   le traitement est **nécessaire à l’exécution d’une mission d’intérêt public** ;

   le traitement est **nécessaire aux fins d’intérêts légitimes**, par exemple à des fins de protection de la santé en ce compris la santé publique, de protection sociale, de prévention de la fraude, de marketing direct… [↑](#footnote-ref-4)
5. Les autres données sensibles sont les suivantes : données à caractère personnel qui sont manifestement rendues publiques par la personne concernée ; le traitement est nécessaire à la constatation d’un droit en justice ou lorsqu’un tribunal agit dans le cadre de sa fonction juridictionnelle ; le traitement est nécessaire pour des motifs d’intérêt public important (il doit être proportionné à l’objectif poursuivi !) ; le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l’appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale ; le traitement est nécessaire pour des motifs d’intérêt public dans le domaine de la santé publique.

   ❖ le traitement est nécessaire à la constatation d’un droit en justice ou lorsqu’un tribunal agit dans le cadre de sa fonction juridictionnelle ; le traitement est nécessaire pour des motifs d’intérêt public important (il doit être proportionné à l’objectif poursuivi !) ; le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l’appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale ; le traitement est nécessaire pour des motifs d’intérêt public dans le domaine de la santé publique. [↑](#footnote-ref-5)
6. <http://ec.europa.eu/newsroom/article29/news-overview.cfm> [↑](#footnote-ref-6)