FICHE D'INFORMATION

L'APPLICATION DU RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES AU SEIN DE L'ASBL

Mise à jour : octobre 2026
Création : 03 décembre 2025 - Ismérie Colussi Corte
Contact : **helpdesk@fass.be**
Destinataires : **membres**
Confidentiel : **non**
Objectif : **Information**
Secteurs concernés : **Tous secteurs**
Commission paritaire concernée : **Toutes CP**

Préambule

Le RGPD est entré en vigueur en Belgique le 25 mai 2018. Il s'applique à tout organisme basé au sein de l'UE ou qui s'adresse à des résidents de l'UE et qui traite des données personnelles dans le cadre de ses activités professionnelles, en ce compris les ASBL.
Il vise à **protéger les individus** des traitements de données personnelles abusives et à **responsabiliser les entreprises et pouvoirs publics** qui traitent des données personnelles. Le RGPD harmonise le droit européen en la matière, assurant ainsi une protection égale sur tout le territoire de l'Union Européenne.

Cette fiche a pour objectif de clarifier les principes généraux du Règlement Général sur la Protection des Données (RGPD) et les obligations qui incombent aux ASBL en la matière.

1. Termes utilisés dans la législation 2
   1.1. Donnée personnelle 2
   1.2. Donnée sensible 2
   1.3. Traitement de données personnelles 2
2. Acteurs impliqués 2
   2.1. L'Autorité de Protection des Données (APD) : 2
   2.2. Le responsable du traitement des données : 3
   2.3. Le·a référent·e RGPD 3
   2.4. Le·a Délégué·e à la Protection des Données (DPO) 3
3. Principes généraux du traitement des données 4
4. Obligations de l'employeur en matière de conformité au RGPD 4
   4.1. Le Registre des Activité des Traitements (RAT) 4

4.2. Documents relatifs à la protection de la confidentialité 5
4.3. Documents relatifs à la sécurisation des données.....6
5. Délais de conservation des données.....7
5.1. Documents financiers.....7
5.2. Documents relatifs aux ressources humaines 7
5.3. Certaines données liées à la sécurité sociale.....7
5.4. Documents de santé.....8
6. Plus d'infos.....8

1. Termes utilisés dans la législation

Quelques termes sont utiles à connaitre pour comprendre les obligations imposées par le RGPD :

1.1. **Donnée personnelle :** toute information permettant d'identifier directement ou indirectement une personne (Art 4, 1). Par exemple, le nom, l'adresse, l'âge, une photographie, etc.

1.2. **Donnée sensible** : donnée bénéficiant d'une protection accrue, compte tenu de la spécificité de l'information et qui ne peut donc être traitée que dans des cas très spécifiques comme un motif d'intérêt général ou pour la sauvegarde des intérêts vitaux de la personne (Art 9 (2)). Par exemple, les données de santé d'une personne, son orientation et/ou sa vie sexuelle, son statut social ou administratif ou encore son appartenance syndicale ou politique.

1.3. **Traitement de données personnelles :** on parle de traitement des données dès lors que des données personnelles sont collectées (Art 4, 2)). Cela inclus également leur enregistrement, utilisation, conservation ou transfert à un partenaire externe. Pour un·e coordinateur·rice d'ASBL, ce traitement concerne à la fois les données des bénéficiaires, mais également des salarié.es et, le cas échéant, des bénévoles.

2. Acteurs impliqués

La législation distingue différents acteurs, exerçant chacun un rôle dans la gestion du traitement des données :

2.1. **L'Autorité de Protection des Données (APD)** : organe de contrôle indépendant chargé de veiller au respect des principes fondamentaux de la protection des données à caractère personnel. Ceci dans différents domaines, tels que l'intelligence artificielle, le droit à l'image, l'accès aux données figurant sur la carte d'identité électronique, etc.1 L'APD est chargée du contrôle du respect de la législation en matière de protection des données et doit être avertie lors d'une fuite de données.

[1] https://www.autoriteprotectiondonnees.be

2.2. **Le responsable du traitement des données :** c'est toujours l'employeur ou son représentant (Organe d'Administration) qui est juridiquement responsable de la conformité au RGPD.

2.3. **Le·a référent·e RGPD** : l'organe d'administration peut désigner, au sein du personnel, une ou plusieurs personnes chargées de la mise en œuvre du RGPD. Il s'agit souvent de membres des RH (collecte et stockage de données du personnel) et/ou du service IT (sécurisation informatique). Dans les petites structures, c'est souvent la coordination/direction qui exécute ces tâches.

2.4. Le·a Délégué·e à la Protection des Données (DPO)[2]

Lorsque l'activité est **financée à plus de 50% par un organisme public** ou **que la gestion est soumise au contrôle des autorités publiques**[3], la désignation d'un.e DPO est obligatoire.

Missions principales :

- Accompagner la mise en œuvre du RGPD
- Conseiller sur les politiques de confidentialité et les pratiques en matière de traitement de données personnelles
- S'assurer que l'ASBL respecte les principes et obligations du RGPD
- Informer, former et sensibiliser l'employeur et les travailleur·ses sur les exigences du RGPD
- Servir de point de contact pour l'Autorité de Protection des Données (APD)

La nomination du·de la DPO n'a pas de forme spécifique. Mais l'usage veut que sa nomination soit actée dans un procès-verbal de l'Organe d'Administration.[4]

Le·a DPO peut-être :

- **Interne** : un·e employé.e de la structure choisi·e en fonction de ses connaissances en droit et en matière de protection des données ainsi que de sa capacité à accomplir les missions du DPO. Cependant, aucun diplôme ou certification spécifique n'est nécessaire pour être désigné·e DPO. La fonction de DPO est incompatible avec l'exercice d'un poste décisionnel au sein la structure, afin d'éviter les conflits d'intérêts et de garantir son indépendance (art. 38 RGPD)
- **Externe** : consultants indépendants (sociétés privées, avocats) pratiquant des tarifs variables selon les services fournis

Le·la DPO doit être enregistré·e auprès de l'Autorité de Protection des Données, via la plateforme en ligne. Ses coordonnées doivent être facilement accessibles dans les documents de politique de confidentialité, sur le site Internet, dans le règlement de travail et autres supports d'informations.

---

[2] Ou DPR, en français, moins couramment utilisé

[3] Article 5 § 3 de la loi belge du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, concernant ce qui constitue une "autorité publique".

[4] Le PV de l'OA mentionne généralement : Le nom du·de la DPO ; son statut interne (membre du personnel) ou externe (consultant indépendant) ; la date de nomination ; un rappel de son indépendance effective et de ses missions.

3. Principes généraux du traitement des données

Le traitement de données personnelles doit suivre un certain nombre de **principes** énumérés dans la législation afin d'en garantir la protection (Art 5).

- Le traitement des données doit être :
  - **Licite**, c'est-à-dire avoir une base légale (consentement de la personne, exécution d'un contrat, intérêt légitime, etc.[5])
  - **Loyal**, c'est-à-dire qu'il doit traiter les données de manière correcte et sans tromper la personne
  - **Transparent**, c'est-à-dire que la personne doit être clairement informée et à l'avance des données collectées, de leur finalité et de la façon dont elles seront utilisées

- Le traitement des données doit également respecter certains principes, à savoir :
  - **La limitation des finalités** : les données collectées doivent être utilisées uniquement pour le but défini au moment de la collecte des données
  - **La minimisation des données** : la collecte doit être limitée à ce qui est nécessaire et pertinent aux finalités du traitement
  - **L'exactitude des données** : les données doivent être tenues à jour et les données inexactes/obsolètes doivent être supprimées
  - **La limitation de conservation** : les données doivent être conservées le moins longtemps possible. Dès que le but du traitement est atteint, elles doivent être supprimées[6]
  - **L'intégrité et la confidentialité** : les données traitées doivent être sécurisées du mieux possible afin de prévenir une violation

L'employeur est responsable du respect de ces principes et doit être en mesure de le prouver auprès de l'APD. Dans le cas contraire, il s'expose à des sanctions.

4. Obligations de l'employeur en matière de conformité au RGPD

En cas de contrôle de la conformité au RGPD, il sera demandé à l'employeur de présenter un **dossier de suivi du traitement des données personnelles**, constitué des documents suivants :

4.1. Le Registre des Activité des Traitements (RAT)[7]

La tenue de ce registre est une obligation formelle du RGPD[8]. Il recense les informations dont l'ASBL dispose et le traitement qui en est fait : données traitées, sources et destinataires (interne ou externe), base légale en justifiant le traitement et la conservation de ces données, mesures de sécurité mises en place pour les protéger, etc. Il constitue le document qui vous sera demandé en priorité en cas d'audit des autorités compétentes (APD) et doit être mis à jour régulièrement.

[5] Pour le détails des bases légales, voir l'article 6 du RGPD
[6] Voir la partie 3 pour les délais de conservation selon les finalités.
[7] Vous trouverez un exemple modifiable dans la partie "Outils" de cette fiche.
[8] Article 30 du RGPD.

4.2. Documents relatifs à la protection de la confidentialité

- **Politique de confidentialité**

Il s'agit d'un document global reprenant de manière synthétique la raison de la collecte des données, leur(s) destination(s), la sécurité mise en place pour les protéger et les conserver. Il doit être facilement accessible, notamment via le site internet, et peut être consulté à la demande.

- **Engagement de confidentialité**

Il s'agit d'un formulaire officiel transmis par l'Autorité de Protection des Données. Chaque travailleur.se (au sens large : salarié.e, indépendant.e, étudiant.e, volontaire) ayant accès à des données personnelles de bénéficiaires et/ou de travailleur·ses doit impérativement signer ce document.

- **Droits des usager·ères et droits des travailleur·ses**

Il s'agit d'un document standard reprenant les droits des usager·ères et des travailleur·ses dans le cadre du traitement, de l'accès, de la modification et de la transmission de leurs données. Il doit être facilement accessible et idéalement affiché dans les lieux fréquentés par les usager.ères (salle d'attente par exemple).

- **Consentement**

  - Travailleur·ses

Document reprenant tous les points pour lesquels l'ASBL est susceptible d'avoir besoin du consentement spécifique du·de la travailleur·se pour pouvoir effectuer le traitement de ses données. Tous·tes les travailleur·ses doivent impérativement le compléter.

  - Usager·ères

Document reprenant tous les points pour lesquels l'ASBL est susceptible d'avoir besoin du consentement spécifique du bénéficiaire pour pouvoir effectuer le traitement de ses données.
Tous les bénéficiaires doivent impérativement le compléter.

  - Candidat.es (facultatif)

Message type de réponse à adresser aux personnes qui ont candidaté lors d'un recrutement et dont on souhaite conserver les données dans une base de recrutement.
Il est également possible de requérir le consentement du.de la candidat·e quant à l'éventuel partage de sa candidature avec une autre structure qui recrute.

  - Autres

Les personnes auxquelles des communications sont envoyées (listes d'envoi pour une Newsletter, par exemple) doivent être informées de la possibilité de se désabonner.

4.3. Documents relatifs à la sécurisation des données

- **La politique de sécurité**

Il s'agit d'un document reprenant très précisément les mesures de sécurité mises en place par l'ASBL. Il n'est en aucun cas public et ne doit être partagé qu'avec les sous-traitants en vertu du principe de coresponsabilité établie par le RGPD.

- **Engament/charte de sécurité**

Il s'agit d'un document reprenant toutes les mesures de sécurité mises en place dans l'ASBL. Il doit être signé par les travailleur·ses de l'ASBL. Il n'est pas public et doit être conservé de manière sécurisée (sur un serveur, sous clé, etc.).

- **Règles en matière de sous traitance**

Sont compris comme sous-traitants les services auxquels l'association a recours pour remplir son objet social et qui traitent des données personnelles. Par exemple, le SEPPT, le secrétariat social, l'hébergeur du site Internet ou un organisme de formation.

En tant de responsable du traitement de données personnelles dans le cadre de ses activités, l'employeur doit s'assurer que les sous-traitants respectent le RGPD.

Pour éviter tout risque pour l'ASBL d'être considérée comme responsable en cas de fuite de données chez un sous-traitant, une clause imposant au sous-traitant le respect du RGPD dans le cadre des activités de traitement de données dont l'ASBL est dépositaire doit être inclue dans le contrat de sous-traitance. De son côté, le sous-traitant doit vous communiquer sa propre politique de sécurité.

- **Procédure en cas de fuite des données**

La **fuite de données** désigne "tout incident entraînant perte, destruction, altération, divulgation non autorisée ou accès à des données personnelles " (par exemple, l'envoi de données à la mauvaise personne, un piratage du serveur, etc.).

En cas de fuite de données, il faut notifier l'Autorité de Protection des Données dans les 72h via le portail en ligne. Cette notification doit décrire la nature de la violation, les personnes concernées par cette violation et les mesures prises en réaction à cette violation. Dans certains cas les plus graves, dans lesquels la fuite présente un risque élevé pour les droits des personnes concernées, il faudra également notifier directement celles-ci (par mail, courrier postal ou tout autres moyens adaptés).

Le **registre/cahier des incidents** permet d'assurer la traçabilité des mesures mises en place par l'ASBL pour traiter les incidents et éviter qu'ils ne se reproduisent à l'avenir. Il recense :

- Les risques pouvant mettre à mal la sécurité des données tant des travailleur·ses que des usager·ères
- L'ensemble des fuites de données dont l'ASBL a été victime, qu'elles soient accidentelles (par ex. perte de clés, de données ou de mots de passe) ou malveillantes (par ex. vol, piratage informatique)

- **Contrôle de l'Autorité de Protection des Données (APD) et sanctions**

En cas de contrôle, l'inspecteur examinera :

- Un exemplaire vierge de chacun des documents mentionnés ci-dessus
- Le Registre d'Activités de Traitement (RAT) complété et mis à jour
- Le registre/cahier des incidents
- La politique de sécurité signée par les sous-traitants
- La politique de sécurité des sous-traitants signée par l'ASBL

En cas de manquement au RGPD, les conséquences les plus probables sont (Art 58) :

- **L'ordre de se mettre en conformité** dans un certain délais
- **La limitation temporaire du traitement des données** : c'est la sanction la plus fréquemment appliquée par l'APD (art. 58). Dans ce cas de figure, l''ASBL ne peut plus utiliser les informations détenues tant que la mise en conformité n'aura pas été effectuée

Lors de manquements graves - violations multiples, manquements persistants, absence de coopération avec l'APD ou refus d'exécuter une mesure corrective - l'ASBL peut faire l'objet d'une **limitation définitive** du traitement et/ou peut être sanctionnée d'**amendes** administratives (Art 83).
En cas d'action intentée devant les tribunaux, l'ASBL risque une amende pénale[9].

5. Délais de conservation des données

Le principe de limitation de conservation des données implique de supprimer les données quand elles ne sont plus utilisées dans le cadre duquel elles ont été récoltées (accompagnement d'un bénéficiaire terminé, candidatures non retenues, etc.).

En Belgique, la conservation des archives pendant une période déterminée est une obligation légale et administrative pour les ASBL, afin notamment d'assurer une traçabilité de leurs activités.

5.1. Documents financiers (journaux comptables, factures, bilans annuels, etc.) : **7 ans** à compter de la clôture de l'exercice auquel ils se rapportent, conformément au Code des Sociétés et Associations (CSA) et à la législation fiscale.

5.2. Documents relatifs aux ressources humaines (contrats de travail, salaires, et autres informations sociales) : maximum **5 ans.**

5.3. Certaines données liées à la sécurité sociale nécessitent une conservation plus longue :

- Les documents relatifs aux cotisations sociales doivent être conservés pendant **7 ans** (déclarations DIMONA, fiches de rémunération et fiches fiscales, justificatifs des paiements de sécurité sociale)
- Les documents relatifs aux accidents de travail doivent être conservés pendant au minimum **10 ans** et parfois jusqu'à 30 ans (en fonction de la prescription de matière de responsabilité civile ou d'assurance)

[9] Les cas restent très rares, l'ADP recommande de passer par d'autres méthodes (médiations, demande d'information) et réserve les plaintes pour les cas plus graves, voir :
https://www.autoriteprotectiondonnees.be/citoyen/agir/introduire-une-plainte

- Les données qui peuvent avoir un impact sur les droits à la pension (périodes de travail, interruptions, congés sans solde, crédit-temps, etc.) doivent être conservées **jusqu'à la pension** voire plus, puisque ces informations peuvent être utilisées très tardivement

5.4. Documents de santé (dossiers des patients) : 30 ans[10]

6. Plus d'infos

- Règlement Général sur la Protection des Données (RGPD)
- Droits des personnes concernant leurs données personnelles (Site de l'APD)
- Toolbox APD (surtout pour le DPO)
- Sur l'espace membre de la FASS :
  - Kit RGPD (FdSS) : outils, trames et modèles pour constituer le dossier relatif au RGPD
  - Addendum au contrat avec Microsoft (boite mail Outlook)
  - Webinaire partie 1 et 2 + diaporama

[10] art. 35 de la loi du 22 avril 2019 relative à la qualité de la pratique des soins de santé