**Mise en œuvre du RGPD**

1. **L’asbl identifie les données à caractère personnel qu’elle traite**

Une donnée est à caractère personnel quand elle se rapporte 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.

Une **donnée est sensible** quand elle concerne l’origine raciale ou ethnique, la santé, les données génétiques ou biométriques ou les opinions politiques et religieuses.

**Un traitement**, c’est : la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Dans une asbl, exemples de données à caractère personnel traitées :

* Données qui se rapportent aux travailleurs salariés (nom, prénom, adresse, numéro de registre national, etc.) pour les obligations légales en matière de droit du travail
* Données relatives aux membres adhérents, aux bénéficiaires, aux publics (nom, prénom, e-mail, adresse, etc.) pour inviter, informer, etc.
* Données relatives à des prestataires de services, des fournisseurs (nom, prénom, e-mail, tél, etc.) pour démarcher, commander, conventionner, etc.
* Données relatives aux bénévoles (nom, prénom, adresse, tél, e-mail, etc.) pour les solliciter, les défrayer, etc.

**2. L’asbl établit une politique de confidentialité**

L’asbl doit fournir certaines informations aux personnes concernées, comme l’identité du sous-traitant et la manière dont il utilisera les données. Ces informations sont généralement communiquées sous la forme d’une déclaration de confidentialité.

Il faut aussi communiquer le fondement légal du traitement de données et les délais pendant lesquels l’asbl conserve les informations, préciser si elle échange des données en dehors de l’Union européenne et prévoir la possibilité pour la personne concernée de porter plainte auprès de la Commission vie privée si elle estime que ses données à caractère personnel sont traitées à tort.

Ces informations doivent être communiquées de manière concise, dans une langue compréhensible et claire.

**3. L’asbl informe les personnes physiques de leurs droits**

Le RGPD prévoit notamment les droits suivants pour la personne concernée :

* information et accès aux données à caractère personnel
* rectification et suppression des données
* objection à l’encontre de pratiques de marketing direct
* objection à l’encontre de prises de décision automatisées et de profilage
* portabilité des données

Cette information se fait : par affichage, par une mention sur le site web ou tout autre support de communication, par courrier, etc. Chaque asbl doit estimer la manière la plus appropriée d’informer.

Cette information permettra à la personne physique :

* De savoir que ses données à caractère personnel sont traitées
* Pourquoi elles sont traitées
* Comment elle peut y mettre un terme
* Comment elle peut à tout moment prendre connaissance des données à caractère personnel que l’asbl traite

**4. L’asbl identifie les fondements sur base desquels elle traite les données à caractère personnel**

**6 fondements légaux** sont prévus pour collecter une donnée :

* Obligation légale ;
* Obligation contractuelle ;
* Autorité publique ou agissant en tant que tel ;
* Intérêts légitimes ;
* Intérêts vitaux ;
* Consentement (**fondement subsidiaire aux 5 autres**)

Aucun autre fondement n’est autorisé par le RGPD. Dans chaque situation, le responsable doit «raccrocher» ses traitements à l’un de ces six critères.

**5. L’asbl demande le consentement si c’est nécessaire**

Le consentement doit être libre, spécifique, éclairé et univoque.

Le consentement doit également se révéler par une manifestation active de l’accord. En d’autres termes, le consentement ne peut pas être déduit tacitement ou à partir d’une case cochée préalablement ou d’une absence d’action.

Le RGPD précise que le responsable du traitement doit être en mesure de démontrer que le consentement a été donné.

**6. L’asbl met en place le régime spécial pour les enfants**

Le RGPD offre une protection spéciale aux données à caractère personnel d’enfants, en particulier dans le contexte de services commerciaux par Internet tels que les réseaux sociaux. En bref, si l’asbl collecte des données **d’enfants âgés de moins de 16 ans**, un parent ou un tuteur devra donner son consentement pour que le traitement de données soit licite.

Le consentement doit être contrôlable et le cas échéant, la déclaration de confidentialité doit être rédigée en des termes compréhensibles pour les enfants.

**7. L’asbl évalue ses contrats existants et les adapte si besoin**

Évaluez vos contrats existants, principalement avec des sous-traitants, et apportez les changements nécessaires.

Un « sous-traitant » est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement. C’est le cas des entreprises d’hébergement sur des serveurs ou du « cloud » comme Microsoft, Google, Facebook, Apple, … -> vérifier que le contrat est conforme au RGPD

En cas d’outsourcing, il est également important d’évaluer si les mesures de sécurité qui étaient prévues dans les contrats existants sont toujours adéquates et répondent aux exigences du RGPD.

*Remarque : l'outsourcing est une pratique qui consiste à externaliser vers un prestataire spécialisé certaines tâches dans le domaine du marketing et de la relation client.*

**8. L’asbl établit son registre de traitement des données à caractère personnel**

Cette obligation ne s’impose pas à tous les organismes. Le registre est obligatoire pour toutes les ASBL composées de plus de 250 employés sauf si le traitement comporte un risque pour les droits et libertés des personnes, des données sensibles ou des données relatives à une condamnation pénale.

Néanmoins, le registre est vivement conseillé (notamment par la Commission de Protection de la Vie Privée) pour toutes les organisations dans la mesure où c’est le premier élément à mettre en place pour être conforme et savoir quelle donnée l’organisation traite.

Le registre des activités de traitement se tient sous une forme écrite et électronique et doit être remis à l’autorité de contrôle sur simple demande.

**Faites l’inventaire minutieux des données à caractère personnel que vous conservez, notez quelle est leur provenance et les personnes avec lesquelles vous les avez partagées.**

Le registre mentionne :

* Qui traite les données à caractère personnel (nommer la personne dans l’asbl qui les traite)
* Quelles catégories de données à caractère personnel sont traitées
* Pourquoi elles sont traitées, les finalités (voir les 6 foncements légaux)
* Quels sont les destinataires (secrétariat social, pouvoir subsidiant, etc.)
* Les délais de conservation (durée du traitement, délai de prescription)
* Les mesures de protection (antivirus, mot de passe, back-up, armoire fermée à clé, mise sous alarme du bâtiment, etc.)

**9. L’asbl prévoit des procédures adéquates pour éviter et traiter les fuites de données**

1. Prévoir des procédures adéquates pour détecter, rapporter et analyser des fuites de données à caractère personnel (exemples : protection IT, système de sécurité organisationnelle)
2. Informer directement la personne concernée faisant l’objet de la fuite de données quand la violation est susceptible d’engendrer un risque élevé pour les droits et libertés de la personne physique (par exemple, quand la fuite peut donner lieu à des pertes financières personnelles).
3. Signaler la fuite à la Commission vie privée dans les 72 heures si la personne concernée risque de subir une quelconque forme de dommages, par exemple suite à un vol d’identité ou une violation d’une obligation de secret.
4. Obliger, sur le plan contractuel, les sous-traitants et/ou responsables conjoints à relayer toute information relative à une violation des données.

**10. L’asbl désigne un délégué à la protection des données si besoin ou si obligatoire**

Les responsables du traitement et le sous-traitant désignent un délégué à la protection des données lorsque :

* Le traitement est effectué par une **autorité publique ou un organisme public**, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle ;
* Les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un **suivi régulier et systématique à grande échelle** des personnes concernées ;
* Les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à **grande échelle** de catégories particulières de **données sensibles** et de données à caractère personnel relatives à des condamnations pénales.

Le délégué à la protection des données peut être un membre du personnel du responsable du traitement ou du sous-traitant, ou exercer ses missions sur la base d'un contrat de service.

Le responsable du traitement ou le sous-traitant publient les coordonnées du délégué à la protection des données et les communiquent à l'autorité de contrôle.