Inventaire et registre des traitements : Définitions

Ce document reprend les définitions des termes et concepts utilisés dans le modèle d'inventaire et de registre à compléter dans le cadre de la mise en œuvre du plan d'action développé par la CESSoC (Feuilles « Inventaire » et « Registre – à dupliquer »).

Légende

La couleur de la ligne précédant les définitions permet de repérer la feuille à laquelle se rapporte la définition.

- *Désigne une définition se rapportant à la feuille « Inventaire »*
- *Désigne une définition se rapportant à la feuille « Registre – à dupliquer »*
- *Désigne une définition se rapportant aux deux feuilles : « Inventaire » et « Registre – à dupliquer »*

La numérotation des définitions correspond à la numérotation des cases du tableur Inventaire-Registre pour une utilisation simplifiée.

Imprimez ce document et garder le à votre disposition pour remplir l'inventaire et le registre.

1. Catégorie de traitement

Par traitement, le RGPD entend « *toute information ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel telles que 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.* »

Nous avons choisi de catégoriser les traitements proposés à l'inventaire selon les différents types de lien entre votre association et les personnes concernées (membres de l'association, travailleurs, …).

2. Nom du traitement

Nous proposons une liste de noms de traitements. À vous de choisir les lignes qui conviennent à votre pratique de terrain et de créer autant de lignes (et de noms de traitement) que de traitements présents au sein de votre institution.

3. Date de création

Date de création du traitement.

4. Date de mise à jour

Dernière mise à jour du traitement. Cette date ne renvoie pas au moment de la dernière modification d'une donnée dans le traitement, mais la date à laquelle la procédure du traitement a été modifié pour la dernière fois.

> ***P.ex. :*** *la date à laquelle le responsable de traitement a décidé de ne plus demander la date de naissance des participants, la date à laquelle le responsable de traitement a décidé de modifier la durée de conservation des données traitées, ...*

5. Responsable du traitement

« La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données à caractère personnel. »
Dans la majeure partie des cas, il s'agira de l'ASBL représentée par son CA, sauf quand celle-ci intervient comme sous-traitant pour le compte d'une autre personne morale ou physique, elle-même responsable de traitement.

👉 Cette case doit être remplie pour chaque traitement.

6. Personne de référence interne

En interne, vous pouvez désigner une ou plusieurs personne(s) physique(s) par traitement.
Cette case n'est pas obligatoire, mais elle vous permet d'identifier rapidement la personne en charge de la gestion du traitement au sein de l'association.

> ***P.ex. :***
>
> *- la personne qui connaît le mieux l'ensemble des processus internes, ou celle qui connaît le mieux un ou plusieurs processus spécifiques : le responsable des ressources humaines pour le traitement des données des travailleurs, le coordinateur, …*
>
> *- un binôme juriste – informaticien.*

7. Sous-traitant

« La personne physique ou morale, autorité publique, service ou organisme qui traite des données à caractère personne pour le compte du responsable de traitement. »

> ***P.ex. :*** *les secrétariats sociaux, les fournisseurs de services cloud pour le stockage de données, une société informatique pour la gestion des bases de données, ...*

👉 À ne remplir que si vous transmettez les données personnelles à un sous-traitant ou si vous agissez vous-même comme sous-traitant.

Pensez également, lorsque vous faites appel à un sous-traitant ou agissez vous-même comme sous-traitant, à définir par écrit les responsabilités des deux parties par rapport au traitement des données, p.ex. dans le cadre de la convention de service qui lie le sous-traitant à votre association (v. Étape 6 du plan d'action CESSoC).

8. Responsable(s) conjoint(s)

Il se peut que plusieurs personnes physiques ou morales déterminent conjointement les finalités et les moyens du traitement des données à caractère personnel.

> ***P.ex. :*** *bases de données développées et tenues à jour conjointement dans le cadre d'un projet mené en partenariat avec une autre association.*

👉 À ne remplir que si d'application.

Pensez également si vous gérez des données personnelles conjointement à définir par écrit les responsabilités des deux parties par rapport au traitement des données.

9. Finalité principale du traitement

Objectif principal de la base de donnée contenant des données personnelles. Les données récoltées ne pourront être utilisées que dans le cadre de la finalité affichée. Cette finalité servira notamment à déterminer la pertinence du traitement et du délai d'effacement des données conservées.

> ***P.ex :***
>
> *- n'est pas pertinente, dans une base de données dont la finalité principale est la gestion des membres de l'AG, une colonne prévoyant des données médicales, à moins que l'association regroupe des patients dont elle défend les intérêts.*
>
> *- est pertinent un délai d'effacement de 5 ans pour des données dont la finalité principale est la gestion du personnel car il correspond au délai de prescription des éventuelles demandes des travailleurs. Ce même délai de 5 ans n'est par contre bien trop élevé pour une base de données dont la finalité principale est l'envoi d'une newsletter.*

Vous trouverez sur la feuille "Exemples" une liste exemplative de finalités de traitement. Nous avons tenté d'être exhaustif, mais n'hésitez pas d'ajouter des finalités propres à votre organisation interne.

Attention : certaines finalités (***p.ex.*** *marketing direct*) peuvent induire des obligations supplémentaires lorsqu'elles sont exercées à grande échelle.

Les éventuelles finalités secondaires seront spécifiées sur la feuille registre là où elles sont applicables.

10. Finalité secondaire du traitement

Outre la finalité principale reprise à l'inventaire des traitements, le traitement de données peut avoir une ou plusieurs finalités secondaires.
Vous trouverez sur la feuille "Exemples" une liste exemplative de finalités secondaires de traitement. Ces finalités secondaires sont principalement liées à l'organisation de votre association. Nous n'y avons donc pas lié de menu déroulant sur le feuille "Registre", afin de vous laisser un choix total dans la détermination de vos objectifs secondaires de traitement.

11. Transfert de données UE / Hors UE

La liste des pays de l'UE se trouve sur la feuille "Exemples".

☞ Remplir avec oui ou non.

12. Taille de l'ASBL : plus de 250 ETP

Dans la législation européenne, et notamment le RGPD, les travailleurs se comptent en "nombre d'unités de travail par année", notion qui peut être assimilée à la notion d'équivalent temps plein en droit belge.

Sont considérés comme travailleurs tous les salariés et toutes les personnes travaillant pour l'association sous un lien de subordination moyennant une rémunération. Seront donc considérés comme des travailleurs : les travailleurs art. 17, des travailleurs mis à disposition, les travailleurs art. 60, ...

À l'inverse, les volontaires (absence de rémunération) ou les indépendants fournissant un service, même régulier (pas de lien de subordination) ne sont pas pris en compte comme travailleurs.

13. Données sensibles

LE RGPD s'applique pour toute information se rapportant à une personne physique identifiée ou identifiable. Toutefois, il fixe une protection supplémentaire pour les données sensibles qu'il énumère aux articles 9 et 10.

Sont considérées comme sensibles,
- les données à caractère personnel qui révèlent l'**origine** raciale ou ethnique, les **opinions politiques**, les **convictions religieuses** ou **philosophiques** ou l'**appartenance syndicale**
- 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** d'une personne physique
- les données à caractère personnel relatives aux **infractions pénales** et aux infractions ou aux mesures de sûreté connexes.

Les trois premières catégories de données sensibles ne peuvent être traitées que lorsqu'une série de conditions sont réunies (p.ex. consentement de la personne, obligations découlant du droit du travail et de la sécurité sociale, …). La dernière catégorie bénéficie d'une protection accrue, étant entendu que les données relatives aux infractions pénales et aux infractions ou aux mesures de sûreté connexes ne peuvent être traitées que sous le contrôle de l'autorité publique ou si le traitement est autorisé par le droit belge ou européen moyennant des garanties appropriées pour les droits et libertés des personnes concernées.

14. Risques pour les droits et libertés des personnes

Prendre en considération pour ce point tous les traitements susceptibles d'engendrer des dommages physiques, matériels ou un préjudice moral (pour plus de détails, voir plan d'action Étape 4).

> ***P.ex. :***
>
> *- le traitement peut donner lieu à une discrimination, à un vol ou une usurpation d'identité, à une perte financière, à une ateinte à la réputation, à une perte de confidentialité de données protégées par le secret professionnel, ou à tout autre dommage économique ou social important*
>
> *- le traitement concerne des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions philosophiques, l'appartenance syndicale, ainsi que des données génétiques, des données concernant la santé ou des données concernant la vie sexuelle ou des données relatives à des condamnations pénales et à des infractions, ou encore à des mesures de sûreté connexes*
>
> *- le traitement sert à créer ou utiliser des profils individuels en évaluant le rendement au travail, la situation économique, la santé, ...*
>
> *- le traitement porte sur des données à caractère personnel relatives à des personnes physiques vulnérables, en particulier les enfants.*

15. Traitement occasionnel

Un traitement sera *"occasionnel"* lorsqu'il se produit à intervalles irréguliers et peu fréquents, par opposition à un traitement habituel.

> ***P.ex. :***
>
> *- **n'est pas** un traitement occasionnel le traitement de données lié à la gestion du personnel régulier de l'association.*
>
> *- **est** un traitement occasionnel la liste des participants à un événement non récurrent ou peu fréquent lorsque les noms (et autres paramètres permettant l'identification) sont utilisés pour l'enregistrement des présences le jour même avant d'être anonymisés ou supprimés à l'issue de l'événement.*

16. Autorité publique ou mission d'intérêt public

Il s'agit des autorités nationales, régionales ou locales et des organismes de droit public. Le Groupe de Travail européen chargé de l'application du RGPD recommande la désignation d'un DPO pour les organisations privées chargées d'une mission d'intérêt public.

Ni le RGPD, ni le Groupe de Travail chargé de son application ne donnent de définition de ce qu'ils entendent par "autorité publique" ou "mission d'intérêt public".

Tous deux se contentent de renvoyer vers le droit national. Le RGPD ne crée donc pas d'obligation de désignation d'un DPO pour ces organisations.

En Belgique, nous attendons toujours une loi d'exécution du RGPD qui donnerait une définition plus précise de ces notions. Toutefois, le projet de loi n'a toujours pas été transmis au parlement au moment de finaliser cet outil (fin avril 2018).

En l'état de la législation belge fin avril 2018, l'on peut considérer que les associations de la CP 329 ne sont ni des autorités publiques, ni chargées de missions d'intérêt public à quelques rares exceptions près.

17. Activité de base => suivi régulier + à grande échelle

- Sélectionnez "oui" si l'activité de base de l'association consiste dans les traitements de données qui du fait de leur nature, de leur portée et/ou de leur finalité exigent un suivi régulier, systématique et à grande échelle des données des personnes concernées.

Il faut entendre par
- **Activité de base** : l'activité liée à la réalisation de l'objet social de l'association *(**p.ex. :** la tenue d'une liste de destinataires des programmes d'un centre culturel fait partie de l'activité de base, les listes des jeunes inscrits dans une unité scoute fait partie de l'activité de base, ...)*. A l'inverse, les activités d'appui (***p.ex. :** gestion du personnel, des fournisseurs de bureau, ...)* ne sont pas des activités de base.

- Lorsque les seuls traitements systématiques, réguliers et à grande échelle concernent les activités d'appui, sélectionnez "non".

- **À grande échelle** : le RGPD ne définit pas ce qu'il faut entendre par "à grande échelle". Tout au plus l'exposé des motifs propose certains critères possibles, comme le nombre de personnes concernées par rapport à une population concernée, la durée ou la permanence de l'activité de traitement. Les exemples proposés dans les recommandations émises par le groupe de travail européen relatif au RGPD (traitement d'informations de voyage de personnes qui se déplacent en transports en commun dans une ville déterminée, traitement de données de clients dans le cadre des activités courantes d'une compagnie d'assurance ou d'une banque, ...) semblent exclure la grande majorité des associations actives dans le secteur socioculturel.

- Ne cochez "oui" que si les activités de base de votre association exigent un suivi régulier, systématique et à grande échelle des personnes concernées.

18. Délégué à la protection des données (DPD) / Data Protection Officier (DPO)

Le DPD ou DPO est une personne interne ou externe à votre organisation chargée de veiller au respect du RGPD dans votre association.
Le RGPD prévoit une série d'hypothèses dans lesquelles il faut en désigner un.

- Répondez par oui ou par non aux colonnes Q et R pour déterminer si l'association est obligée de désigner un DPD ou DPO.

À partir du moment où vous êtes obligé de désigner un DPD ou DPO pour un type de traitement, la désignation devient obligatoire pour tous les traitements dans l'association.

Sur base de notre analyse des activités du secteur de la CP 329, nous concluons qu'il n'y aura que peu d'associations concernées par cette obligation (sous réserve de la définition retenue pour la notion d'"autorité publique", v. ci-dessus).

Si, néanmoins, il vous semble sur base de l'inventaire que vous devriez désigner un délégué à la protection des données, nous vous conseillons de vous adresser à votre fédération.

19. Délai d'effacement

Il vous appartient de définir la durée de conservation des données. Choisissez un délai suffisamment long pour correspondre aux finalités que vous avez assignées au traitement visé et aux éventuelles obligations juridiques qui en découlent (v. également définition de finalité principale du traitement).

> ***P.ex. :** Une action en récupération de salaires d'un travailleur peut porter sur des faits datant de jusqu'à 5 ans avant la fin de la relation de travail et peut donc justifier un délai d'effacement qui soit d'un peu plus de 5 ans après la fin de la relation de travail.*

> ***P.ex. :*** *Le contenu d'une réponse à une offre d'emploi n'est pertinent que pendant une courte période après la fin de la procédure de recrutement (nouvelle procédure de recrutement si le candidat sélectionné ne convient pas au poste, éventuel recours d'un candidat s'estimant victime d'une discrimination, ...). Le délai d'effacement ne devrait donc pas excéder 1 an après le recrutement du candidat recherché.*

20. Licéité du traitement

Complétez ici la base légale qui permet le traitement des données concernées (v. menu déroulant). Les bases légales sont énumérées de manière limitatives dans le RGPD. Le traitement sera licite s'il remplit au moins une des conditions suivantes :

- **Donnée nécessaire à l'exécution d'un contrat** : pour autant que le caractère nécessaire des informations traitées puisse être démontré. Pour l'établissement du contrat ou la prestation des services convenus, ce fondement juridique suffit comme justification.
  > ***P.ex. :*** *besoin du numéro de compte de tous les volontaires pour verser les défraiements convenus.*
- **Obligation légale :** La loi ou les décrets et ordonnances ainsi que leurs arrêtés d'exécution peuvent contraindre une organisation à recueillir une série de données.
  > ***P.ex. :*** *obligation de fournir des listes de participants dans le cadre d'un arrêté déterminant les formalités de subventionnement, obligation de fournir aux banques des informations sur la composition du Conseil d'Administration dans le cadre de la lutte contre le blanchiment d'argent, ...)*
- **Sauvegarde des intérêts vitaux de la personne concernée** : ce fondement ne peut concerner que les urgences où le traitement des données peut avoir un impact sur des questions de vie ou de mort
- **Tâches d'intérêt général ou exercice de l'autorité publique** : en l'absence de définition de l'autorité publique par une loi belge et tant que la loi transposant le RGPD en droit belge n'a pas été votée, les associations du secteur socio-culturel n'effectuent pas de tâches liées à l'exercice de l'autorité publique. Elles peuvent éventuellement réaliser des tâches d'intérêt général (***p.ex. :*** *des recherches scientifiques, ...*)
- **Intérêts légitimes du responsable de traitement ou d'un tiers** : ce fondement est le plus faible de tous. Veillez à expliciter de quel intérêt il s'agit et de l'équilibrer avec le droit à la confidentialité des personnes concernées.
- **Consentement de la personne concernée** : lorsque la licéité du traitement n'est fondée par aucune des bases légales qui précèdent, vous devez demander le consentement de la personne concernée. Assurez-vous que le consentement de la personne concernée soit explicite et couvre toutes les données demandées (v. Étape 7 du plan d'action de la CESSoC et ses annexes).