



RGPD

Règlement Général pour la Protection des Données

Notions théoriques

Sommes-nous concernés ?

Ces dispositions s'appliquent à toute personne physique ou personne morale, y compris les asbl, qui traite des données personnelles de personnes physiques :

- que le traitement de ces données soit automatisé en tout ou en partie ;
ou
- que ce traitement ne soit pas automatisé MAIS que les données soient contenues ou appelées à figurer dans un fichier.

A retenir :

Les données sont collectées dans un cadre professionnel :

- n'est donc pas visée la collecte de données à caractère personnel effectuée par une personne physique dans le cadre d'une activité strictement personnelle ou domestique.

Les données récoltées concernent des personnes physiques, pas des personnes morales (entreprises, asbl,...) :

- une base de données de fournisseurs avec une adresse courriel « info@ », sans mention de personnes physiques, ne relève pas du RGPD ;
- par contre, une base de données de fournisseur avec une adresse mail « jean.emar@ » relève du RGPD. Ainsi, le seul fait de mentionner dans la base de données le nom du contact professionnel au sein de l'entreprise « x » suffit pour considérer que l'on collecte des données à caractère personnel.

Les données récoltées concernent des personnes physiques identifiées ou identifiables :

- la notion de personne identifiée est assez simple : le nom, le numéro de registre national ;
- la notion de personne identifiable vise l'hypothèse où la personne peut être identifiée, directement ou indirectement, notamment par référence à un identifiant (exemples : une donnée de localisation, un numéro d'identification, une adresse IP, un numéro d'affiliation, une plaque minéralogique,...).

Les données récoltées ne doivent pas nécessairement être automatisées :

- disposer d'informations personnelles « sur papier », dans un classeur avec les fiches classées (quel que soit le mode de classement, par ordre alphabétique par exemple), suffit pour relever du RGPD ;
- seules des données personnelles récoltées « sur papier » et non classées ne relèvent pas du RGPD.

La notion de traitement des données est très large :

- elle vise 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, l'interconnexion, la limitation, l'effacement ou la destruction des données.

Qui sommes-nous ?

On peut être responsable de traitement OU sous-traitant.

Le **responsable de traitement** est celui qui détermine les finalités et les moyens d'un traitement de données à caractère personnel.

Le **sous-traitant** est celui qui traite les données à caractère personnel pour le compte, sur instruction et sous l'autorité d'un responsable de traitement.

Un exemple :

Un informaticien « externe » peut être :

- le sous-traitant d'un client (votre asbl) ;
- le responsable de traitement pour son propre fichier de clientèle.

A retenir :

Il nous semble que, dans tous les cas, nous sommes responsables de traitement.

Par contre, si la mise en place d'une éventuelle base informatique est effectuée par un service informatique externe, ce service devient notre sous-traitant puisqu'il va traiter des données à caractère personnel sous notre autorité.

De quoi sommes-nous responsables ?

Le responsable de traitement doit veiller à ce que les données à caractère personnel soient :

- traitées de manière licite, loyale et transparente ;
- collectées pour des finalités déterminées, explicites et légitimes ;
- adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités poursuivies ;
- exactes et, si nécessaire, tenues à jour ;
- conservées pendant une durée ne dépassant pas celle nécessaire au regard des finalités poursuivies ;
- traitées de façon à garantir une sécurité appropriée.

Le responsable de traitement doit apporter les mêmes garanties de la part de tout sous-traitant auquel il fait appel.

Ligne générale conductrice : le principe d'« accountability »

Notion d'accountability :

Il s'agit d'une obligation de rendre compte et d'expliquer, avec une idée de transparence et de traçabilité permettant d'identifier et de documenter les mesures mises en œuvre pour se conformer aux exigences issues de la réglementation RGPD.

Le responsable de traitement doit être à même de démontrer que, pour chaque donnée à caractère personnel, il a respecté les 6 principes repris à la page précédente.

L'obligation d'accountability implique, pour le responsable de traitement :

- de prendre les mesures efficaces et appropriées afin de se conformer au RGPD ;
- d'apporter la preuve, sur demande de l'Autorité de Protection des Données (APD – anciennement CPVP), que les mesures appropriées ont été prises.

A retenir :

Le responsable de traitement devrait garder une trace écrite de toutes les réflexions qui l'ont amené à prendre telle ou telle décision :

- pourquoi a-t-il pris telle mesure de sécurité ?
- pourquoi n'a-t-il pas désigné de délégué à la protection des données (DPD) ?
- quelle méthodologie de traitement des données a-t-il choisie et pourquoi ?
-

Etape prioritaire : tenue d'un registre des activités de traitement

La tenue de ce registre est obligatoire dans les entreprises de moins de 250 travailleurs SSI :

- le traitement de données à caractère personnel N'est PAS occasionnel ;

OU

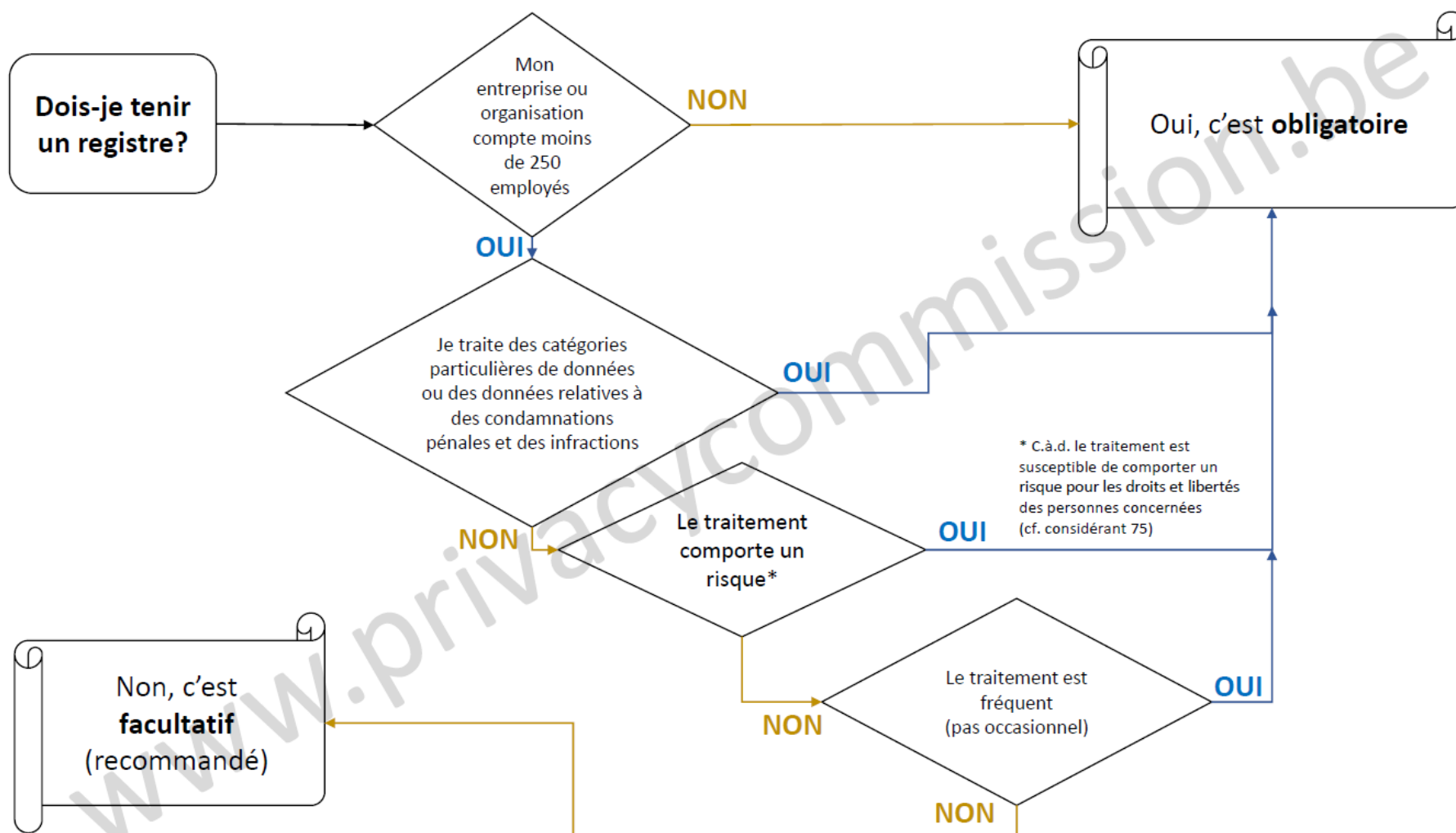
- le traitement porte sur des données à caractère personnel particulières, à savoir :
 - o des données qui révèlent l'origine raciale ou ethnique ;
 - o des données qui révèlent les opinions politiques ;
 - o des données qui révèlent les convictions religieuses ou philosophiques ou l'appartenance syndicale ;
 - o des données génétiques ;
 - o des données biométriques aux fins d'identifier une personne physique de manière unique ;
 - o des données concernant la santé ;
 - o des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique ;

OU

- le traitement de données à caractère personnel est susceptible de comporter un risque pour les droits et les libertés des personnes concernées ;

OU

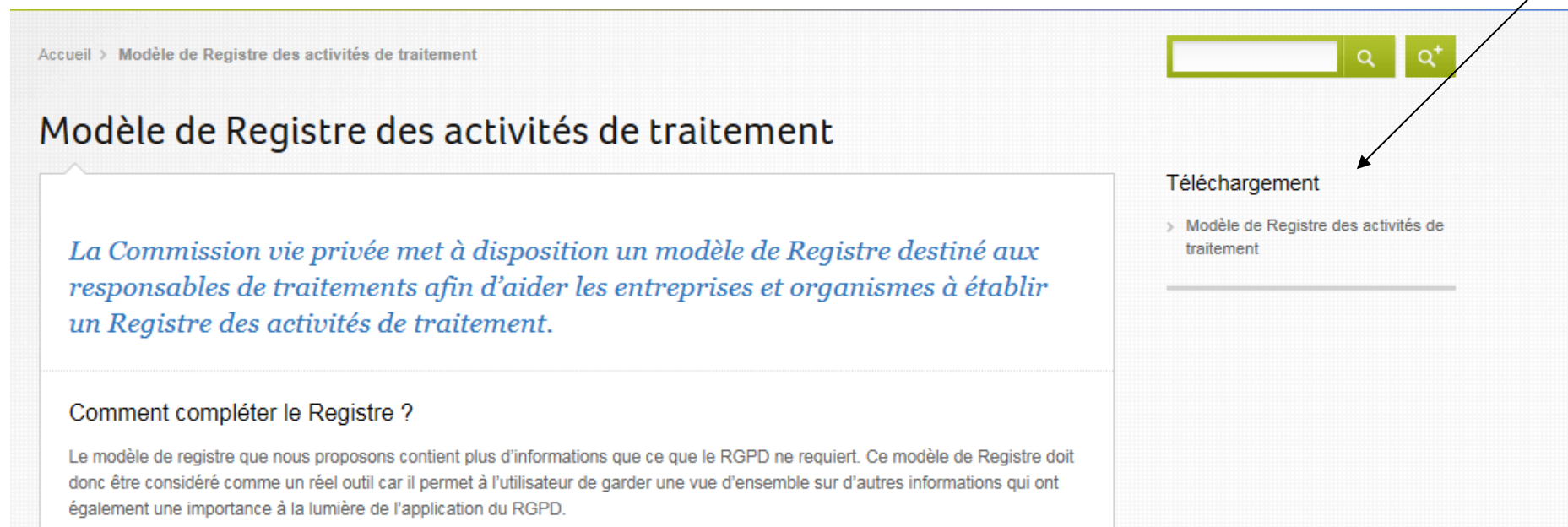
- le traitement de données à caractère personnel concerne des condamnations pénales, des infractions ou des mesures de sûreté connexes.



Le registre des activités de traitement doit reprendre :

- le nom et les coordonnées du responsable du traitement ;
- les finalités du traitement ;
- une description des catégories de personnes concernées et des catégories de données à caractère personnel ;
- les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées ;
- dans la mesure du possible, les délais prévus pour l’effacement des différentes catégories de données ;
- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles.

Un modèle de registre est disponible sur le site de la CPVP (bientôt APD – Autorité de Protection des Données) : <https://www.privacycommission.be/fr/canevas-de-registre-des-activites-de-traitement>



Accueil > Modèle de Registre des activités de traitement

Modèle de Registre des activités de traitement

La Commission vie privée met à disposition un modèle de Registre destiné aux responsables de traitements afin d'aider les entreprises et organismes à établir un Registre des activités de traitement.

Comment compléter le Registre ?

Le modèle de registre que nous proposons contient plus d'informations que ce que le RGPD ne requiert. Ce modèle de Registre doit donc être considéré comme un réel outil car il permet à l'utilisateur de garder une vue d'ensemble sur d'autres informations qui ont également une importance à la lumière de l'application du RGPD.

Téléchargement

- > Modèle de Registre des activités de traitement

Quelles sont les « bases de données » pour lesquelles un traitement paraît nécessaire ?

Nous pouvons identifier au moins 4 types de données différenciées :

- celles relatives aux stagiaires ou aux jeunes ou aux bénéficiaires ou aux primo-arrivants ou aux sportifs,... pour lesquels le pouvoir subsidiant demande la récolte de données précises ;
- celles relatives aux travailleurs salariés, au conseil d'administration, à l'assemblée générale, aux bénévoles ;
- celles relatives aux fournisseurs ;
- celles relatives aux clients types « commerciaux », aux partenaires.

Pour être licite, le traitement de données à caractère personnel doit remplir au moins une des conditions suivantes :

- **la personne concernée a consenti au traitement** de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ;
- le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ;
- **le traitement est nécessaire au respect d'une obligation légale** à laquelle le responsable du traitement est soumis ;
- 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 ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;
- le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers.

Exemple de la différence entre le traitement d'une donnée dans le cadre d'une obligation légale ou dans le cadre d'un consentement :

L'employeur dispose de l'adresse de ses travailleurs. Pour les utiliser, il peut / doit se référer :

- à une obligation légale pour le calcul des frais de déplacement domicile – lieu de travail ;
- à un consentement écrit du travailleur pour lui envoyer une invitation à aller fêter tel jubilé dans telle autre structure.

Droit des personnes physiques faisant l'objet d'un traitement de données à caractère personnel

Droit d'accès et de rectification des données

A tout moment, la personne physique doit disposer des éléments lui permettant de prendre contact avec l'institution qui a récolté et conservé ses données personnelles pour y avoir accès et les rectifier si nécessaire.

Droit de portabilité

Il s'agit d'un droit complémentaire au droit d'accès aux données le concernant.

C'est le droit, pour la personne concernée :

- de recevoir les données la concernant dans un format structuré, couramment utilisé et lisible par une machine (PC) ;
- et si c'est techniquement possible, d'obtenir que les données soient directement transmises à un autre responsable de traitement (ceci ne vise que les données dont le responsable de traitement dispose en raison du consentement écrit de la personne concernée et pour lesquelles le traitement est effectué à l'aide de procédés automatisés).

Droit à l'oubli numérique (ou droit à l'effacement)

La personne concernée a le droit d'obtenir l'effacement de ses données « dans les meilleurs délais » dans les cas suivants :

- les données à caractère personnel ne sont plus nécessaires au regard des finalités poursuivies ;
- elle retire le consentement sur lequel est fondé le traitement ;
- elle s'oppose au traitement de ses données à des fins de prospection ;
- les données ont fait l'objet d'un traitement illicite ;
- les données ont été collectées dans le cadre de l'offre directe de service à un enfant de moins de 16 ans.

Délégué à la protection des données (DPD) : obligation ou non ?

La désignation d'un délégué à la protection des données (DPD) n'est **obligatoire que dans trois cas** :

- le traitement des données à caractère personnel est effectué par une autorité publique ou un organisme public ;
- les activités de base du responsable de traitement 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 (profilage) ;
- les activités de base du responsable de traitement consistent en un traitement à grande échelle de catégories particulières de données (données sensibles – voir ci-avant).

A retenir :

- on n'est pas toujours obligé de recourir à un DPD ;
- si nous le faisons, ce DPD peut être interne ou externe à la structure ;
- si nous désignons un DPD, il faut cadrer :
 - o les tâches à exécuter ;
 - o le temps dont il dispose pour les exécuter ;
 - o les responsabilités respectives ;
 - o le secret professionnel / devoir de discrétion ;
 - o la protection du DPD ;
 - o les sanctions éventuelles si le cadre n'est pas respecté.

La sous-traitance

Pour rappel, le **sous-traitant** est celui qui traite les données à caractère personnel pour le compte, sur instruction et sous l'autorité d'un responsable de traitement.

Sans entrer dans les détails, gardons à l'esprit que le recours à un sous-traitant suppose un cadre juridique précis fixant les responsabilités respectives du responsable de traitement et du sous-traitant.

Entrée en vigueur

L'entrée en vigueur de ces nouvelles dispositions, dont nous n'avons proposé qu'une esquisse, est le 25/05/2018.