Création et mise à jour d'un registre de traitements

https://www.leben-avocats.com https://virtual-dpo.fr

Qu'est ce qu'un registre de traitements ?

L'article 30 du RGPD prévoit une obligation de tenir un registre des traitements de données personnelles effectués par les responsables de traitement.

Ce registre doit contenir :

- L'identité des parties qui traitent les données (responsable de traitement, sous-traitant etc.);
- Les catégories de données traitées;
- La finalité du traitement, les personnes ayant accès aux données et leurs destinataires;
- La durée de conservation de ces données;
- La manière dont elles sont sécurisées.

La création d'un registre au-delà d'être obligatoire permet d'avoir une vision claire du niveau de conformité de son organisation avec la réglementation en matière de données personnelles.

Le registre est un outil de suivi permettant de relever les failles ou les incohérences dans le traitement de données personnelles. Il est également utile pour démontrer sa conformité aux autorités ou à des partenaires commerciaux. Dans ce dernier cas, le registre servira de base pour répondre aux questions des partenaires et rédiger d'éventuels documents contractuels.

Deux volets distincts

Le RGPD impose de consigner les activités de traitement réalisées par l'organisation pour son propre compte, en tant que responsable de traitement, et pour le compte de ses clients, en tant que sous-traitant.

Il convient donc de distinguer ces deux types de traitements en les consignant dans des registres distincts ou de les séparer visiblement au sein du même document (par exemple, deux feuilles distinctes de classeur Excel).

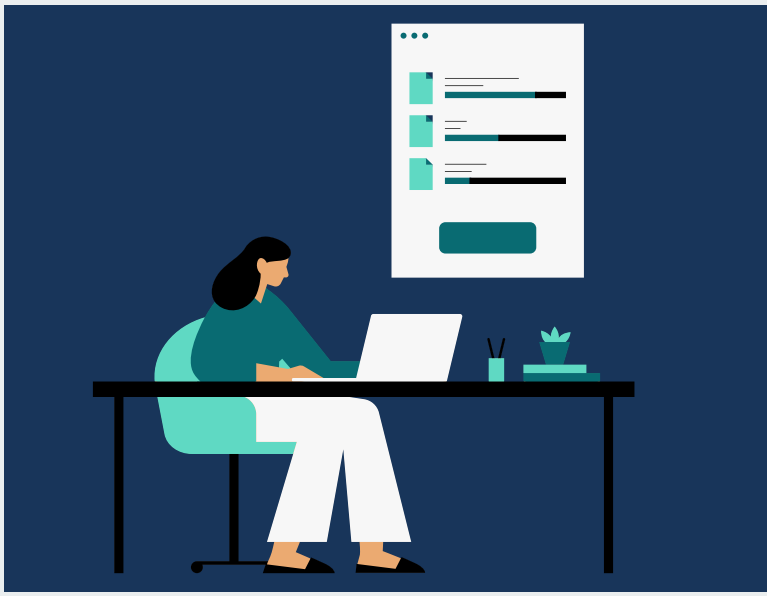
Le registre du responsable de traitement

Il convient de consigner dans un registre les traitements effectués en tant que responsable de traitement, à savoir les traitements effectués pour le compte de l'organisation et sous son contrôle.

Certains traitements de données seront communs à toutes les entreprises, en particulier ceux reposant sur des obligations légales ou comptables.

Par exemple, les traitements de données des salariés en relation avec les déclarations aux organismes sociaux.

D'autres peuvent être spécifiques à l'entreprise et traduire les traitements propres à son activité.



Le registre du sous-traitant

Le registre des activités de traitement effectuées en sous-traitance recense les activités de traitement mises en place par l'organisation pour le compte de ses clients.

Il conviendra de détailler chaque type de traitement effectué usuellement par l'organisation pour le compte de tiers.

Le registre devra également contenir, le cas échéant, les sous-traitants auxquels a recours l'organisation elle même, appelés sous-traitants ultérieurs ou de second rang.

Constituer un registre

Déterminer et répertorier les finalités et les données traitées

Pour créer un registre, il convient dans un premier temps, d'établir une cartographie des flux de données de l'entreprise.
Il est nécessaire de répertorier chaque type de données personnelles traitées, et la raison de ce traitement, qui peut s'exprimer en termes génériques, par exemple :

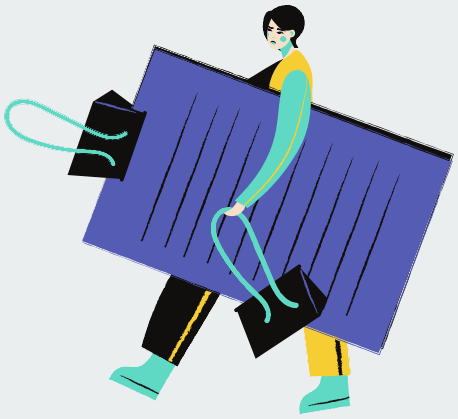
"*Suivi des demandes support*" est une finalité de traitement.

Associer les différents départements de l'entreprise ainsi que les responsables ou managers de ceux-ci à cet exercice permet une retranscription fidèle des traitements de données effectués au sein de l'organisation.

Choisir et mettre en place des durées de conservation des données

Le principe de minimisation des données personnelles limite la durée pendant laquelle elles peuvent être conservées.
Il faut mener une réflexion sur la durée de conservation des données, qui dépendra de leur type et de leur usage.

L'organisation devra prendre en compte ses besoins, la durée pendant laquelle les données demeurent pertinentes ou utiles à son activité, les durées de conservation recommandées par la Cnil et les obligations légales de conservation.
Par exemple: les documents comptables doivent être conservés pendant 10 ans.



Mettre régulièrement le registre à jour

Une fois les éléments nécessaires réunis et le registre des traitements établis, il est primordial de le tenir à jour.

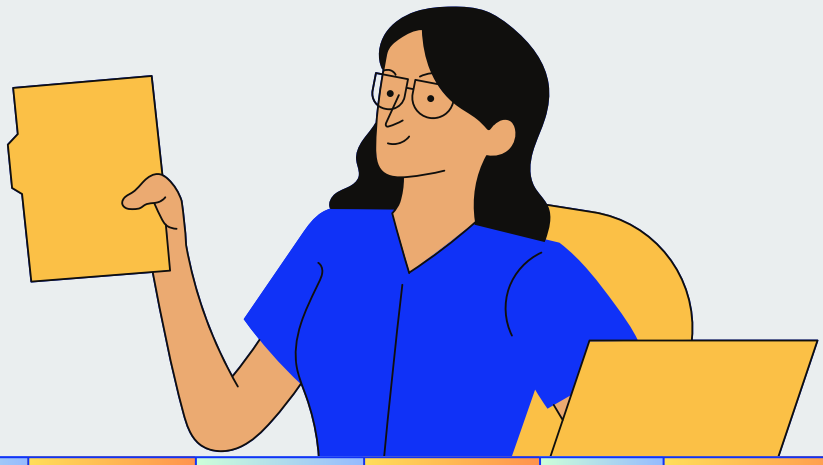
Il convient alors, selon les évolutions internes, d'ajouter les nouvelles activités de l'organisation qui supposent le traitement de données, de tenir à jour la liste des sous-traitants de l'entreprise, s'assurer que les durées de conservation sont respectées et les adapter, le cas échéant.

Quelle forme peut prendre un registre de traitement ?

La forme du registre des traitements est libre, il convient néanmoins de garder à l'esprit qu'il doit permettre aux autorités et aux partenaires de constater la conformité de l'organisation avec le RGPD et au personnel de l'entreprise de l'adapter simplement en cas d'évolution des traitements des données. Il doit donc être complet mais également suffisamment clair et simple à manipuler.

Le registre est en général établi sous forme de tableau. Un modèle est proposé par la CNIL. Il existe également des logiciels spécialisés.

Un exemple est reproduit ci-dessous à titre d'illustration, pour un traitement dont la finalité est le "suivi des demandes de support", les éléments figurant dans le tableau varient selon les entreprises.



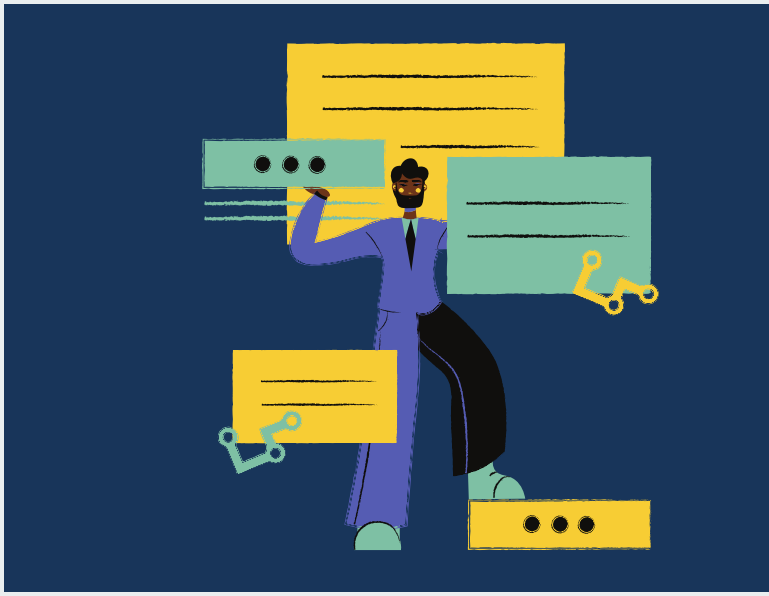
FINALITÉ	DATE DE MISE EN ŒUVRE	NATURE DES DONNÉES	PERSONNES CONCERNÉES	FONDEMENT	DESTINATAIRE	DONNÉE SENSIBLE	DURÉE DE CONSERVATION	DURÉE DE L'ARCHIVAGE INTERMÉDIAIRE	SOUS-TRAITANTS PRINCIPAUX
Suivi des demandes de support	1/01/2023	Nom, prénom, adresse e-mail, contenu de la demande.	Clients et représentants personnes physiques des clients	Contrat	Département IT Service client	Non	Jusqu'au traitement de la demande	5 ans	Outils de support
Indiquer l'objectif poursuivi	*Indiquer la date du 1er traitement*	*Lister le type de données*	*Lister les personnes auxquelles appartiennent les données*	*Indiquer la base légale (consentement, contrat, intérêt légitime, obligation légale)*	*Indiquer qui a accès aux données au sein de l'organisation*	*Indiquer si les données ont un caractère sensible*	*Indiquer la durée pendant laquelle les données sont utilisées*	*Indiquer la durée pendant laquelle les données sont conservées avec un accès restreint (en général pour des besoins de preuve)*	*Indiquer si ce traitement suppose le recours à sous-traitant*

S'assurer de la conformité d'un sous-traitant

Rechercher et répertorier

Lorsqu'une organisation fait appel à un sous-traitant pour mettre en place des traitements de données personnelles, elle doit s'assurer de sa conformité avec le RGPD.
L'entreprise qui sous-traite une activité devra définir clairement l'objet de cette sous-traitance (par exemple l'hébergement de services informatiques), les données personnelles susceptibles d'être accessibles, si celles-ci font l'objet d'un transfert hors de l'Union Européenne, et le cas échéant, le mécanisme qui sécurise ce transfert.

Ces éléments se retrouvent parfois dans les documents contractuels (conditions générales, politique de confidentialité, etc.) ou peuvent être directement communiqués par le sous-traitant.



Documenter

Les informations recueillies concernant le sous-traitant doivent être consignées.

Celles-ci peuvent apparaître dans les contrats passés avec les sous-traitants ou dans un document spécifique au traitement des données personnelles mais il peut être utile de les reporter dans un onglet dédié du registre de traitements.

Un registre clair

Prêt à être présenté

Qui atteste de la conformité de l'organisation au RGPD