AVOCATS EN DROIT DES AFFAIRES

# REGLEMENT GENERAL SUR LA PROTECTION DES DONNEES PERSONNELLES (« RGPD ») : LE REGISTRE DES ACTIVITES DE TRAITEMENT

## 1. QU'EST-CE QU'UN REGISTRE DES ACTIVITES DE TRAITEMENT ?

L'article 30 du RGPD impose aux responsables de traitements et aux sous-traitants de mettre en place des registres des activités de traitements effectués sous leur responsabilité (dans le cas du RT) ou pour le compte du RT (dans le cas du ST).

Concrètement, il faudra donc répertorier les activités de traitement de données à caractère personnel.

Ces notions sont entendues très largement.

On entend par traitement : « toute opération 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 »;

Quant aux données à caractère personnel, il s'agit de « toute information se rapportant 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 »; (article 4 du RGPD)

## 2. A QUOI ÇA SERT ?

Ce recensement s'inscrit dans la logique du principe *d'« Accountability »* prévu par le RGPD et qui impose aux entreprises de :

- prendre des mesures efficaces et appropriées afin de se conformer au règlement européen
- et d'apporter la preuve, sur demande de l'autorité de contrôle, que ces mesures ont été prises.

Cela passe notamment par l'obligation de conserver une trace documentaire de tout traitement effectué sous la responsabilité du responsable du traitement ou du sous-traitant.

Ainsi, les obligations de déclarations préalables à la CNIL sont supprimées et remplacées par la tenue de ce registre écrit des activités de traitement (sous format papier ou électronique), qu'il faudra pouvoir présenter aux autorités compétentes en cas de contrôle (article 30 du RGPD).

MARCEAU AVOCATS
71, avenue Marceau – 75116 Paris
Tel: +33 (0) 1 53 57 90 10
Fax: +33 (0) 1 40 70 09 65
http://www.marceau-avocats.com

## 3. TRAITEMENT ET FINALITE ?

Les traitements identifiés dans le registre sont définis en fonction de leurs finalités principales. Un traitement peut être effectué via l'utilisation de plusieurs outils et applications et un outil ou une application peut servir plusieurs finalités. Il ne s'agit pas de faire une fiche par outil/application mais bien par traitement.

Exemple : J'ai mis en place dans mon entreprise plusieurs dispositifs de sécurité : caméra de vidéosurveillance, badges d'entrée pour les salariés. Ces outils collectent des données personnelles. Une fiche pour le traitement « Surveillance des biens et locaux » sera créée dans le registre des activités de la société ayant pour finalités : assurer la sécurité des biens et des personnes, prévenir les risques. Les badges d'entrée remis aux salariés servent également à surveiller les horaires d'arrivée des salariés, ce qui correspond à un autre traitement et fera donc l'objet d'une autre fiche.

## 4. A QUI INCOMBE CETTE OBLIGATION ?

Cette obligation s'impose aux responsables de traitement et aux sous-traitants ainsi qu'à leurs représentants[1] le cas échéant pour les activités de traitements qui sont sous leur responsabilité.

Dans le cas où des représentants ont été désignés, un seul registre commun au représentant et au représenté suffit.

## 5. MEME POUR LES TPE ET PME ?

Le texte prévoit que cette obligation ne s'applique pas à une entreprise ou une organisation comptant moins de 250 salariés.

Toutefois, cette dispense ne s'applique pas si l'entité se trouve dans l'un des cas suivants :

- le traitement est susceptible de comporter un risque pour les droits et libertés des personnes concernées (voir le profilage ou le considérant 75 du RGPD pour des exemples : le traitement peut donner lieu à une discrimination, à un vol ou une usurpation d'identité…)
- le traitement n'est pas occasionnel (exemple : traitement régulier de données lié à la gestion du personnel, des fournisseurs ou de la clientèle, etc.)
- le traitement porte sur des données « sensibles » (les données concernant l'origine raciale ou ethnique, la religion ou les convictions, les opinions politiques ou toute autre opinion, l'appartenance à un syndicat, la santé, la vie sexuelle ou l'orientation sexuelle d'une personne)
- le traitement porte sur des données judiciaires (condamnations pénales et infractions)

En pratique donc, cette dispense est limitée (les traitements sont bien souvent permanents et pas occasionnels).

[1] Lorsqu'un responsable du traitement ou un sous-traitant n'est pas établi dans l'Union Européenne mais se voit quand-même appliquer le RGPD, il doit désigner un représentant légal.

## 6. QUELLES INFORMATIONS DOIVENT FIGURER DANS LE REGISTRE ?

Les informations à faire figurer dans le registre ne sont pas exactement identiques selon que le traitement est effectué par un responsable de traitement ou par un sous-traitant.

Dans l'ensemble, il s'agit des mêmes informations que celles qui devaient être communiquées pour effectuer des déclarations CNIL ou précisées dans le registre du Correspondant Informatique et Libertés (CIL), s'il en existe un au sein de la société. Ci-dessous un tableau qui récapitule les informations à faire figurer pour chaque traitement.

| | Informations à faire figurer | Responsable de traitement | Sous-traitant |
|---|---|---|---|
| **QUI ?** | Nom et coordonnées du responsable de traitement et de son représentant le cas échéant (et DPO le cas échéant) | X | X |
| | Nom et coordonnées du sous-traitant | | X |
| **POURQUOI ?** | Finalités du traitement | X | |
| | Catégories de traitement | | X |
| **QUOI ?** | Personnes concernées et catégories de données concernées | X | |
| **OÙ ?** | Destinataires | X | |
| | Transfert vers un pays tiers ou organisation internationale | X | X |
| **JUSQU'A QUAND ?** | Délais de conservation et d'effacement des données | X | |
| **COMMENT ?** | Description de mesures de sécurité techniques et organisationnelles | X | X |

Il s'agit ici des informations obligatoires qui doivent figurer dans le registre pour chaque traitement, mais il est possible (et conseillé) d'en ajouter[2].

[2] Ainsi, on peut s'étonner que le texte dispose par exemple que le responsable de traitement doive préciser les « finalités du traitement » mais pas les « catégories de traitement » (en pratique, les catégories de traitement seront de toute évidence dans le registre, c'est l'objet même de cette obligation).

# 7. QUELQUES OUTILS

La CNIL et la CPVP (autorité belge) ont élaboré des modèles de registre qui ne sont pas des formats officiels mais constituent toutefois des outils intéressants.

https://www.cnil.fr/fr/cartographier-vos-traitements-de-donnees-personnelles

https://www.privacycommission.be/fr/canevas-de-registre-des-activites-de-traitement

Par ailleurs, les anciennes déclarations CNIL et normes simplifiées peuvent constituer une bonne source d'inspiration en ce qui concerne les éléments à faire figurer dans le registre (exemple : la norme simplifiée NS-048 relative aux fichiers clients – prospects énumère toute une liste de finalités et de données collectées).

MARCEAU AVOCATS
71, avenue Marceau – 75116 Paris
Tel: +33 (0) 1 53 57 90 10
Fax: +33 (0) 1 40 70 09 65
http://www.marceau-avocats.com