MANDIL AVOCATS

Privacy by Design by Default

Fiche n°04 - Février 2020

L'article 25 du RGPD prévoit deux nouveaux principes en vertu desquels les responsables du traitement, avec l'aide de leurs éventuels sous-traitants, doivent prendre les mesures techniques et organisationnelles appropriées pour que :

- **Dès la conception d'un service ou d'un bien nécessitant un traitement de données personnelles, celui-ci soit conforme aux dispositions du RGPD tout au long de son cycle de vie ;**
- **Par défaut, seules les données personnelles nécessaires soient traitées.**

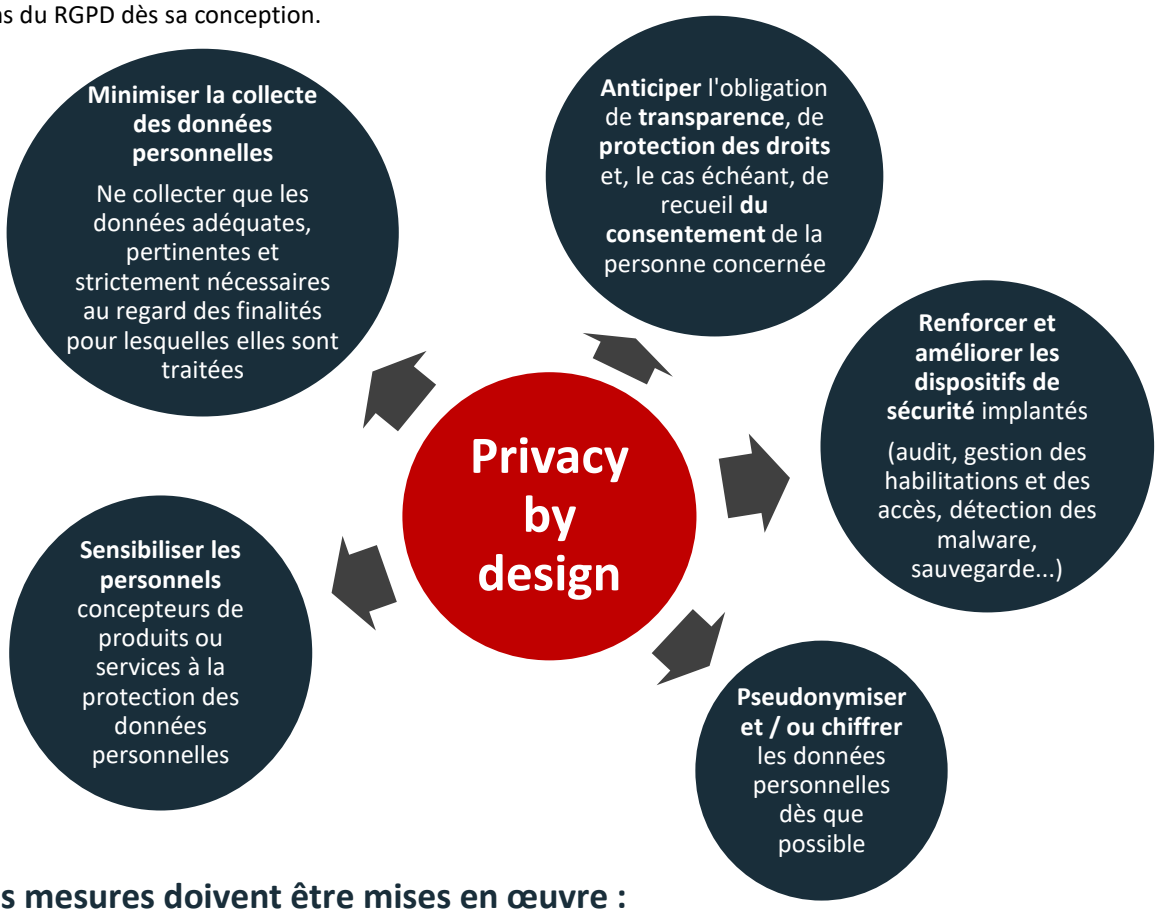
A savoir

Projet de lignes directrices de l'EDPB du 13 novembre 2019

Les autorités européennes (EDPB) ont publié le 13 novembre 2019 leur **projet de lignes directrices** sur les principes de protection des données personnelles dès la conception et par défaut. Celles-ci fournissent des indications sur la manière d'appliquer ces principes en pratique, reconnaissent que les sous-traitants et les fournisseurs de technologies en sont les principaux facilitateurs et incitent l'ensemble des acteurs à en tirer un **avantage concurrentiel**.

I. Le principe de *Privacy by design*

Le responsable du traitement (avec l'aide de ses sous-traitants éventuels) qui conçoit un produit ou un service doit **mettre en œuvre des mesures techniques et organisationnelles** permettant de garantir la conformité de ce service ou produit aux dispositions du RGPD dès sa conception.



Ces mesures doivent être mises en œuvre :

Dès la phase de conception et même de planification d'un bien ou service

Pendant toute la durée du traitement et donc évaluées régulièrement pour rester à jour

Pour déterminer les mesures techniques et organisationnelles appropriées, **les responsables du traitement doivent tenir compte de** :

L'Etat de l'art
Ils doivent se tenir au courant des progrès technologiques et y veiller avec leurs sous-traitants.

Le coût et les ressources nécessaires
Y compris les RH et le coût potentiel des amendes résultant du non-respect du RGPD.

La nature, la portée, le contexte et la finalité du traitement
Notamment pour s'assurer de sa proportionnalité.

Les risques pour les droits et libertés des personnes
Risques d'accès non autorisé, de modification ou de perte des données par exemple.

II. Le principe de *Privacy by Default*

En vertu de ce principe, le responsable du traitement doit adopter des mesures consistant à **limiter, par défaut, le traitement à ce qui est strictement nécessaire**. La limitation peut notamment concerner :

La **quantité de données collectées** (volume, type…)	La **diversité des finalités**	La **durée de conservation** (puis suppression ou anonymisation)	Le **nombre de personnes** habilitées à **accéder** aux données

Exemple d'application du principe de *Privacy by default* : un service en ligne proposant plusieurs niveaux de paramétrage de confidentialité devra être réglé par défaut, lors de l'inscription, sur le niveau le plus protecteur.

A noter

Privacy by design, privacy by default et certification

Les responsables du traitement doivent pouvoir démontrer que les mesures mises en œuvre produisent l'effet souhaité en termes de protection des données : **détermination d'indicateurs clés de performance appropriés (quantitatifs et/ou qualitatifs).**

Les fabricants de produits ou les concepteurs de services peuvent recourir à des mécanismes de certification (labels, marques…) et/ ou adhérer à des codes de conduite qui prévoient la mise en œuvre de mesures techniques et organisationnelles garantissant la protection des données personnelles dès la conception et par défaut.
L'utilisation de ces outils leur permettra de bénéficier d'une présomption de conformité en cas de contrôle par la CNIL.

La certification est une procédure par laquelle un tiers certificateur va donner l'assurance écrite qu'une personne, un produit, un processus ou un service est en conformité avec les exigences d'un référentiel.
La certification est contraignante et doit être renouvelée : elle donne lieu à un contrôle régulier par le tiers certificateur du respect du référentiel via des audits et des examens.
La CNIL peut directement certifier des organismes et agréer des organismes certificateurs ou, selon les cas, choisir de collaborer avec le Comité Français d'Accréditation (COFRAC).

Les codes de conduite sont élaborés par les acteurs professionnels (fédérations, organisations professionnelles) et se composent de bonnes pratiques dans un secteur d'activité donné (durée de conservation, mention d'information, modes opératoires…). Un organisme peut librement adhérer à un code de conduite.
Le RGPD prévoit qu'un organisme tiers sera chargé de contrôler le respect d'un code, lui conférant un caractère contraignant.

MANDIL AVOCATS