

Le service juridique doit s'assurer de la conformité de l'entreprise avec les dispositions du RGPD et notamment concernant les droits des personnes, le principe d'accountability et la mise en place d'un DPO.

DROITS DES PERSONNES

► Il convient de s'assurer que l'entreprise met en place les mesures nécessaires au respect des droits des personnes concernées.

Les personnes (clients, salariés, co-contractants) doivent être **informées de leurs droits et de la manière dont elles peuvent les exercer ainsi que sur les traitements mis en œuvre** (identité du responsable de traitement, finalités, durées, DPO, destinataires).

Cette information passe notamment par la mise en place d'une :

CHARTRE DE PROTECTION

DES DONNÉES

PERSONNELLES

INTERNES



CHARTRE DE PROTECTION

DES DONNÉES

PERSONNELLES

EXTERNES

Les droits de la personne sont :

à destination des salariés

à destination des clients et co-contractants.



Le droit d'accès

Obtention d'information sur ses données traitées et la façon dont elles sont traitées



Le droit de rectification

Rectification des données à caractère personnel la concernant qui sont inexactes



Le droit à l'effacement ou droit à l'oubli

Effacement, dans les meilleurs délais, de données à caractère personnel la concernant



Le droit à la limitation du traitement

Les données à caractère personnel la concernant sont simplement conservées sans autres traitements



Le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé

Y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire.



Le droit d'opposition

Pour les traitements fondés sur une mission d'intérêt public ou sur les intérêts légitimes poursuivis par le responsable de traitement ou un tiers ou à des fins de prospection



Le droit à la portabilité des données

Droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine

Le service juridique doit s'assurer de la conformité de l'entreprise avec les dispositions du RGPD et notamment concernant les droits des personnes, le principe d'accountability et la mise en place d'un DPO.

ACCOUNTABILITY

L'accountability est l'obligation pour un responsable du traitement de rendre des comptes. Elle consiste à apporter les éléments de preuve du respect des dispositions du RGPD. Il s'agit donc de documenter les différentes mesures prises par le responsable du traitement en conformité avec le RGPD.

LES PRINCIPES DE BASE DU TRAITEMENT

Cette documentation porte en premier lieu sur les principes de bases du traitement, à savoir :



Traitement licite, loyal et transparent des données



Finalités déterminées, explicites et légitimes



Données adéquates, pertinentes et limitées au regard des finalités



Données exactes et tenues à jour



Durée non excessive



Sécurité des données.

DOCUMENTATION

Ensuite, il s'agit de disposer des documents suivants :



Le registre des traitements



Les analyses d'impact



DROITS DE LA PERSONNE



La documentation porte également sur les droits de la personne concernée. Il s'agit de conserver :

Les différentes mentions d'information et les modalités de communication des informations et notamment le processus de communication orale des informations

Les modèles de recueil du consentement des personnes concernées ainsi que les supports de recueil du consentement des personnes concernées

Les procédures de gestion des demandes des personnes concernées.

SOUS-TRAITANTS



Pour les relations avec les sous-traitants, il est impératif de conserver les contrats.

FLUX TRANSFRONTIÈRES

En cas de flux transfrontières, les garanties appropriées et les garanties adéquates doivent être conservées. Il s'agit par exemple des règles d'entreprise contraignantes.

Le service juridique doit s'assurer de la conformité de l'entreprise avec les dispositions du RGPD et notamment concernant les droits des personnes, le principe d'accountability et la mise en place d'un DPO.

DATA PROTECTION OFFICER

OBLIGATOIRE



Traitement effectué par une « **autorité publique** » ou par un « **organisme public** »



Lorsque les activités de base du responsable de traitement exigent un **suivi régulier et systématique à grande échelle des personnes concernées**



Lorsque les activités de base du responsable de traitement consistent en un **traitement à grande échelle de catégories particulières de données**



Lorsque les activités de base du responsable de traitement consistent en un **traitement à grande échelle de données relatives à des condamnations pénales et à des infractions**

RECOMMANDÉ

Même lorsque cela n'est pas obligatoire, la désignation d'un DPO est recommandée, il a pour missions de :

Coopérer avec la Cnil

Dispenser des conseils sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données



Informier et conseiller

le responsable du traitement ainsi que les employés qui procèdent au traitement sur leurs obligations

Contrôler le respect du RGPD

Faire office de point de contact pour la Cnil sur les questions relatives au traitement.

i

La désignation du DPO devra être notifiée :

- à la Cnil
- aux salariés
- et aux instances de représentation du personnel.

Les documents d'informations des personnes concernées par les traitements devront également faire mention du DPO et de ses coordonnées.

