

La protection des données personnelles : quel(s) rôle(s) pour l'avocat ?

mercredi 27 avril 2022

INTERVENANTS :

Alexandre LAZAREGUE, Avocat au Barreau de Paris
Sandy MOCKEL, Membre du Conseil de l'Ordre de Paris
Nadine MOKDAD, juriste et DPO de l'Ordre

Introduction

OBJECTIFS

- ✓ Appréhender la protection données à caractère personnel.
- ✓ Comprendre les changement qu'implique le règlement européen EU 2016-679,
- ✓ Historique des textes consacrés à la protection des données.

- 1. Les grands principes du RGPD**
- 2. Les obligations du RGPD**
- 3. Les sanctions de l'autorité de contrôle**
- 4. Les acteurs de la conformité**



Depuis 40 ans*, il fallait respecter la loi Informatique et Libertés

*Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Les 5 principes clés de la protection des données personnelles



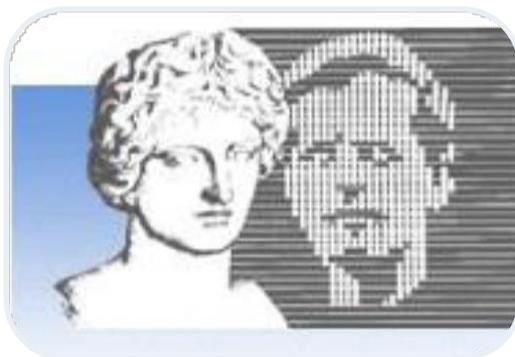
la finalité



la pertinence



la conservation



les droits



la sécurité

**Depuis le 25 mai 2018, il faut être en
conformité avec le Règlement
Général sur la Protection des
données (RGPD)**



Les principes fondamentaux I&L

DONNEE A CARACTERE PERSONNEL

Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.

RESPONSABLE DE TRAITEMENT

Le responsable du traitement est la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens.

LA FINALITÉ

Avant toute collecte et utilisation de données personnelles, l'organisme doit précisément annoncer aux personnes concernées ce à quoi elles vont lui servir.
L'utilisation de ces données est encadrée par la loi.

LA PERTINENCE

Seules les données strictement nécessaires à la réalisation de l'objectif peuvent être collectées

LA CONSERVATION

Une fois que l'objectif poursuivi par la collecte des données est atteint, il n'y a plus lieu de les conserver et elles doivent être supprimées.

LES DROITS

Les personnes disposent des droits auprès de l'organisme qui détient leurs données : un droit d'accéder à ces données, un droit de les rectifier et enfin un droit de s'opposer à leur utilisation

LA SÉCURITÉ

L'organisme doit prendre toutes les mesures nécessaires pour garantir la sécurité des données qu'il a collectées mais aussi leur confidentialité,

Les obligations du RGPD

Pourquoi se conformer à la réglementation ?



C'est une **obligation réglementaire**



C'est un enjeu de **communication** pour les organisations



Les organismes sont de plus en plus **exposés**.



Les données sont des **actifs** fortement convoités et sujets aux vols



Les usagers sont de plus en plus **sensibles à l'exploitation** de leurs données (surveillance, vente de leurs données à des fins commerciales, etc.).



Les **sanctions** en cas de non-conformité ont fortement augmenté

Le principe de licéité du traitement

Les Données personnelles doivent être traitées de manière Licite (Article 5 RGPD).

Le traitement est licite si il est justifié par l'une des Bases/fondements juridiques de l'article 6 du RGPD :

- L' exécution du Contrat ou mesures précontractuelles;
- Le Respect d'un obligation légale à laquelle le Responsable du traitement est soumis;
- La sauvegarde des intérêt vitaux de la personne concernée ou d'une autre personne physique;
- L' exécution d'une mission d' intérêt public;
- L'exécution d'intérêts légitimes par le Responsable de traitement.
- Et à défaut d'autres fondements, le Consentement de la personne concernée.



Les droits des personnes concernées 1/2

RGPD : Renforcement des droits des Personnes

➤ **Droit d'accès**

Vous pouvez demander à un organisme s'il détient des données sur vous et demander à ce que l'on vous les communique pour en vérifier le contenu.

➤ **Droit de rectification**

Vous pouvez demander la rectification des informations inexactes ou incomplètes vous concernant. Il permet d'éviter qu'un organisme n'utilise ou ne diffuse des informations erronées sur vous.

➤ **Droit d'opposition**

Le droit d'opposition vous permet de vous opposer à ce que vos données soient utilisées par un organisme pour un objectif précis

➤ **Droit à limitation**

C'est le droit de demander à un responsable de traitement de « geler » temporairement l'utilisation de certaines de vos données. Concrètement, le responsable de traitement ne devra plus utiliser les données mais devra les conserver.

Inversement, vous pouvez demander directement la limitation de certaines données dans le cas où l'organisme souhaite lui-même les effacer. Cela vous permettra de conserver les données par exemple afin d'exercer un droit.

➤ **Droit à l'information**

Les responsables de traitement doivent informer les personnes concernée des éléments suivant pour traiter les données personnelles : l'identité du responsable du fichier ; la finalité du fichier ; le caractère obligatoire ou facultatif des réponses et des conséquences d'un défaut de réponse ; les destinataires des données ; leurs droits (droit d'accès, de rectification, et d'opposition) ; les éventuels transferts de données vers des pays hors UE

Les droits des personnes concernées 2/2

RGPD : consécration de nouveau droits

➤ **Droit à la portabilité**

La personne concernée a le droit de récupérer les données qu'elle a fournies au responsable de traitement. Ce droit ne peut être utilisé que si le traitement des données est basé sur le consentement de la personne concernée ou sur un contrat.

➤ **Droit à l'effacement/oubli**

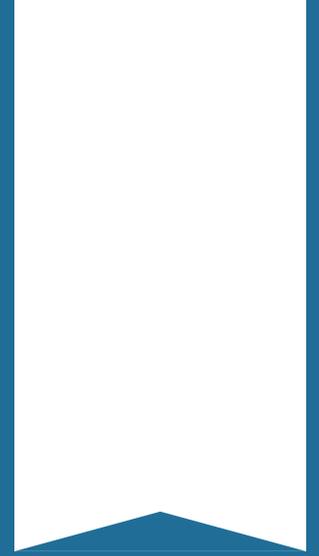
La personne concernée peut demander l'effacement de ses données pour l'un des motifs listés dans l'article 17 du RGPD

➤ **Action de groupe**

Des associations pourront agir en justice pour faire valoir les droits des personnes en matière de protection des données personnelles



Les sanctions



Les sanctions de l'autorité de contrôle 1/2

Violations punies d'une amende maximum de: 10 M€ ou 2% du CA mondial

Collecte et traitement de données superflues ...	Non respect de protection des données dès la conception et par défaut	Absence de contrat avec un sous-traitant de données	Absence de clauses réglementaires au contrat d'un sous-traitant	Choix d'un sous-traitant ne présentant pas de garanties suffisantes	Non enregistrement d'un traitement au registre
Défaut de sécurité et de confidentialité	Absence de garantie que des données sensibles ne sont pas accessibles à des personnes non identifiées	Refus de coopérer avec la CNIL	Défaut de notification à la CNIL et à la personne concernée d'une violation de données	Absence de désignation d'un DPO	Non réalisation de PIA's ou non consultation de la CNIL avant mise en œuvre de certains traitements

Les sanctions de l'autorité de contrôle 2/2

Violations punies d'une amende maximum de: 20 M€ ou 4% du CA mondial

Violation des principes de base	Traitement illicite des données	Absence de recueil de consentement	Information préalable faisant défaut ou non conforme	Absence de mesures facilitant l'exercice des droits	Absence /refus de répondre aux demandes d'exercice des droits
Absence de transparence dans l'exploitation des données	Prise de décision automatisé à impact individuel	Transfert de données hors UE	Non respect d'une injonction de la CNIL	Non respect de l'opposition à la prospection commerciale	Collecte et traitement de données sensibles hors consentement



Les acteurs de la Conformité RGPD

Le délégué à la protection des données (DPO)

Le Data Protection Officer ou DPO, nommé par le Responsable de Traitement, a un rôle de « chef d'orchestre » animant un réseau d'experts métiers (les relais, correspondants ou référents). Il est chargé, avec leur contribution, de mettre en œuvre la conformité RGPD au sein de l'organisme qui l'a désigné.

Les missions du DPO :

- Informer et conseiller le responsable du traitement quand aux obligations en matière de protection des données personnelles
 - Diffuser la « culture Protection des données personnelles » via des actions de sensibilisation et de formation
- Veiller au respect de la Règlementation relative à la protection des données personnelles
 - Intégrer dans chaque projet la protection des données dès la conception
 - Mener des audits de conformité RGPD
- Assurer le principe « d' accountability »
 - Tenir le registre des activités de traitements mis en œuvre au sein de l'organisme
 - Rédiger des analyses d'impact pour les traitements considérés comme sensibles
- Être l'interlocuteur de la CNIL, Rôle d'interface avec les autorités de contrôle
- Gérer les demandes de droit des personnes concernées
- Être en veille constante et adapter l'ensemble des processus et supports aux évolutions législatives
- Produire des rapports annuels sur la protection des données personnelles