TERMES ANGLAIS ET ACRONYMES UTILISÉS DANS CET OUVRAGE

- *Device* : Désigne les différents écrans (mobile, tablette, écran…)
- *Responsive* : Site web multiformat et adapté aux différents écrans
- *Display* : Publicité sur Internet
- CSAT : Score de satisfaction client
- NPS : *Net Promoter Score*
- CES : *Customer Experience Score*
- FAQ : Foire aux questions
- CRM : (*Customer Relation Management*) Gestion de la relation client
- CCM : (*Customer Communication Management*) Gestion de la communication client
- CXM : (*Customer Experience Management*) Gestion de l'expérience client
- *Customer Experience* (CX) : Expérience consommateur
- *User Experience* (UX) : Expérience utilisateur
- *User-centric* : Vision centrée utilisateur
- *Buyer persona* : Cible acheteur
- *Paintpoints* : Irritants ou points de friction
- *Funnel marketing* : Parcours d'achat de l'internaute
- *Wishlist* : Liste de favoris
- SVI : Service vocal interactif
- CTI : Couplage téléphonie informatique
- SEA : (*Search Engin Advertising*) Référencement payant
- SEO : (*Search Engin Optimization*) Référencement naturel
- SXO : *Search Experience Optimization*
- *Homepage* : Page d'accueil
- *Landing page* : Page d'atterrissage liée à un bouton d'action sur Internet
- Liens *backlinks* : Liens sur site Internet naturels entrants par recommandation
- Liens *follow* : Liens de site à caractère non publicitaires
- CTA : (*Call to Action*) Bouton incitant à l'action sur un site
- *Inbound marketing* : Marketing entrant visant à attirer le client par du contenu
- *Content marketing* : Marketing basé sur la qualité des contenus pour séduire
- KPI : (*Key Performance Indicator*) Indicateur d'analyse et de performances
- CTR : (*Clic Through Rate*) Taux de clic
- *Leads* : Prospects sur Internet

SOMMAIRE

Fiche 1 Les données personnelles
Fiche 2 Le traitement d'une donnée personnelle
Fiche 3 Le droit des personnes
Fiche 4 Les obligations du responsable de traitement et du sous-traitant
Fiche 5 Le registre des données personnelles
Fiche 6 L'analyse d'impact relative à la protection des données
Fiche 7 Le délégué à la protection des données (DPO)
Fiche 8 La sécurité des données
Fiche 9 La notification d'une violation
Fiche 10 Les règles des entreprises contraignantes (*Binding Corporate Rules*)
Fiche 11 La transmission de données à des pays tiers autorisés ou à des organisations internationales
Fiche 12 Les codes de conduite
Fiche 13 Les certifications
Fiche 14 Comment se protéger contre les atteintes ?
Fiche 15 La CNIL : autorité de contrôle
Fiche 16 Le Comité européen de protection des données (CEPD)
Fiche 17 Les voies et les recours
Fiche 18 Les responsabilités et les sanctions
Fiche 19 Le RGPD et le respect des droits et des libertés

FICHE 1

LES DONNÉES PERSONNELLES

Un peu d'histoire

L'histoire de la protection des données personnelles s'est déroulée en 3 étapes.

1. La France a été le premier État européen à se doter d'une législation spécifique en matière de protection des données personnelles avec la **loi du 6 janvier 1978 dite « Loi informatique et libertés »**.
2. **La directive 95/46 du Parlement européen et du Conseil en date du 24 octobre 1995** relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel fut transposée en droit interne par la loi du 6 août 2004.
3. **Le règlement 2016/679 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel** et à la libre circulation de ces données dit RGPD a été adopté le 27 avril 2016 et abroge la précédente directive 95/46. Le texte a été transposé en droit interne par la loi du 25 mai 2018.

LE POINT SUR ...

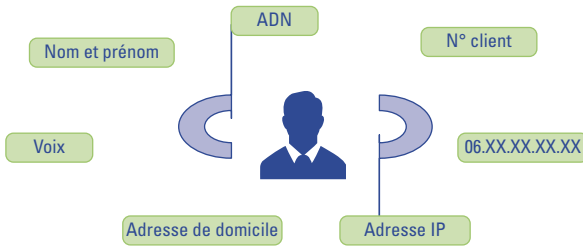
La loi informatique et libertés de 1978

Cette loi pose le principe que « l'informatique doit être au service de chaque citoyen » et « qu'elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'Homme, ni à la vie privée, ni aux libertés individuelles ou publiques » (article 1er).

De quoi parle-t-on ?

- Une donnée personnelle est « toute information se rapportant à une personne physique identifiée ou identifiable ». Il s'agit des données informatisées ou stockées sur des fichiers papiers.

Exemples de données directes et indirectes d'identification d'une personne



- Un **fichier** est un ensemble de données à caractère personnel qui est accessible selon des critères déterminés. Le fichier peut être soit centralisé soit décentralisé, de même, il peut être réparti de manière fonctionnelle ou géographique.
- Le « **Guichet unique** » est un principe selon lequel un groupe ayant des établissements dans plusieurs pays d'Europe, ou une activité dans plusieurs États-membres, peut effectuer ses formalités en matière de traitement des données auprès de l'autorité de l'État-membre dans lequel le groupe a son établissement principal.

Ce qu'il faut savoir …

1. Le RGPD s'applique aux activités ayant recours à un traitement des données à caractère personnel dès lors **qu'un établissement, un responsable de traitement ou un sous-traitant se situent sur le territoire de l'Union**, que le traitement ait lieu ou non dans l'Union. Exemple : les entreprises « GAFAM » telles que Meta (ex-Facebook).
2. L'identification d'une personne peut également être réalisée à **partir du recoupement de plusieurs données** et de leur croisement. Exemple : un homme vivant dans tel village, né telle année et qui est abonné à tel magazine.
3. Un fichier qui ne contient que des données relatives à une entreprise ne constitue pas un traitement de données personnelles.

EXEMPLE

Pass NAVIGO et liberté de circuler anonymement

Dans un avis du 8 avril 2004, la CNIL rappelle à la RATP, gestionnaire des pass NAVIGO, que la circulation dans les transports publics doit pouvoir se faire de manière anonyme. Jusqu'alors cette obligation n'était pas respectée, car les déplacements étaient associés aux numéros des abonnés. Depuis, tout contrôle se fait sur présentation de 2 cartes : l'une nominative comportant les données personnelles de l'abonné et l'autre anonyme retraçant ses déplacements.

Les droits tout au long de la vie

Personne mineure

Une protection renforcée des données personnelles est prévue, notamment s'agissant des activités de marketing et de profilage de consommateurs. Ainsi, le consentement du représentant légal est requis pour les mineurs de moins de 16 ans. En outre, la loi du 7 octobre 2016 prévoit un droit à l'oubli pour les mineurs. Dans un délai réduit d'un mois, le droit à l'oubli permet d'obtenir l'effacement en ligne de ses données personnelles de la personne concernée.

Pour un mineur de moins de 16 ans, le traitement est licite dans la mesure où le consentement est donné par le représentant légal du mineur. Pour un mineur de plus de 16 ans, le traitement est licite lorsque la personne a consenti au traitement de ses données personnelles et ce, pour une ou plusieurs finalités spécifiques.

Par ailleurs, la loi prévoit que l'accès à certains sites ou services sur Internet est réservé aux majeurs, en particulier l'accès aux sites web à caractère pornographique. À cet égard, la CNIL recommande que les mécanismes de contrôle de l'âge soient mis en œuvre par des organismes distincts de l'éditeur du site visité. Ainsi, le site qui vérifie l'âge requis doit connaître l'identité de la personne, mais ne doit pas savoir quel site est visité. À l'inverse, le site visité doit recevoir la preuve de l'âge requis, mais ne doit pas connaître l'identité de la personne.

Personne décédée

S'agissant du droit à la maîtrise des données *post mortem*, la loi du 7 octobre 2016 vient encadrer la succession numérique des actifs du défunt (photos, œuvres, comptes…).

FICHE 2

LE TRAITEMENT D'UNE DONNÉE PERSONNELLE

De quoi parle-t-on ?

Un traitement de données personnelles est une opération ou un ensemble d'opérations portant sur des données personnelles et ce, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, extraction, consultation, utilisation, communication, mise à disposition, effacement, destruction). Par exemple, la collecte des données d'enregistrement des passagers par une compagnie aérienne. Il n'existe aucune distinction entre les formats retenus pour le traitement des données. Ainsi, la loi s'applique à tous les types de traitements qu'ils soient automatisés ou non.

EXEMPLE

Fichiers et Témoins de Jéhovah

Dans un arrêt du 10 juillet 2018, la Cour de justice de l'UE a considéré que la notion de « fichier » couvre « tout ensemble de données à caractère personnel collectées » dans le cadre d'une activité de prédication (en l'espèce, celles de Témoins de Jéhovah) et comportant des noms et des adresses ainsi que d'autres informations concernant les personnes démarchées.

LE POINT SUR ...

Les données exclues du RGPD

- Une activité qui ne relève pas du champ d'application du droit de l'Union.
- Une activité des États-membres qui relève de la liberté, de la sécurité ou de la justice.
- L'activité des autorités compétentes à des fins de prévention et de détection des infractions pénales.
- L'activité d'une personne exercée à titre strictement personnel et domestique.

Les 6 grands principes du traitement de données

1. Un traitement licite, loyal et transparent au regard de la personne concernée

EXEMPLE

Le recueil du consentement

La CNIL recommande que le consentement soit recueilli de manière écrite, comme la signature apposée à la fin d'un formulaire de renseignement.

2. Une collecte pour des finalités déterminées, explicites et légitimes

EXEMPLE

Le bouton « J'aime » de Facebook

La justice allemande a demandé à un site de vente en ligne sur Internet de préciser à ses utilisateurs la finalité du bouton « J'aime » de Facebook. En effet, derrière ce bouton, il existe un puissant système de traitement des données.

3. Un traitement adéquat, pertinent et limité à ce qui est nécessaire au regard des finalités

EXEMPLE

La finalité d'un traitement d'intérêt public

Les données médicales collectées et conservées par un hôpital répondent à une mission d'intérêt public.

4. Des données exactes et si nécessaires tenues à jour

EXEMPLE

Les fichiers Acadomia d'élèves, de parents et d'enseignants

En 2009, la CNIL a constaté la présence de milliers d'informations concernant des élèves, des parents et des enseignants comportant des caractères excessifs et détenues par la société Acadomia.

5. Une conservation sous une forme permettant l'identification des personnes et ce, pendant un délai n'excédant pas celui nécessaire au regard des finalités

EXEMPLE

Le fichier RH d'une entreprise

Dans une entreprise, les données d'un candidat non retenu à l'obtention d'un poste peuvent être conservées pendant 2 années maximum.

6. Un traitement garantissant la sécurité des données à caractère personnel

EXEMPLE

Le niveau de sécurité adapté au risque

Chaque entreprise doit évaluer son niveau de risque en fonction des matériels (nombre d'ordinateurs), des logiciels et des canaux de communication (wifi...) qu'elle utilise.

La légalité du traitement des données

Un **traitement** est considéré comme **licite** si l'une des conditions suivantes est remplie.

- La personne concernée a **consenti** au traitement de ses données.
- Le traitement est **nécessaire à l'exécution d'un contrat** auquel la personne est partie.
- Le traitement est **nécessaire au respect d'une obligation légale.**
- Le traitement est **nécessaire à l'exécution d'une mission de service public.**
- Le traitement est **nécessaire aux fins d'intérêts légitimes** poursuivis par le responsable de traitement.