PINT Avocats

WOOXO
IT security for business continuity

LIVRE BLANC

RÉGLEMENT GÉNÉRAL DE LA PROTECTION DES DONNÉES

COMPRENDRE & AGIR

Ce document vous présente les points essentiels du RGPD pour vous aider à en comprendre les notions

PREAMBULE

Le RGPD (GDPR en anglais) a été approuvé le 27 avril 2016 après 4 ans de négociations par les instances européennes. En France, il remplace la directive de 1995 et la loi Informatiques et Libertés de 1978.
Il est directement applicable à tous les citoyens, organismes et entreprises. Les sanctions sont applicables depuis le 25 mai 2018.

VOUS ETES CONCERNE SI :
VOUS COLLECTEZ OU HEBERGEZ DES DONNEES PERSONNELLES CONCERNANT UN INDIVIDU (FRANÇAIS OU ETRANGER) RESIDANT SUR LE TERRITOIRE DE L'UNION EUROPEENNE.
VOUS ETES RESPONSABLE DE TRAITEMENT DE DONNEES OU SOUS-TRAITANT ETABLI EN UNION EUROPEENNE.

Votre responsabilité vous assigne à utiliser de nouveaux outils de conformité pour recenser les données personnelles dont vous avez la charge.

EN BREF

L'enjeu est de faire du RGPD et de ses contraintes un outil de compétitivité : la sécurité des données est un gage de confiance et de qualité, recherché par les clients et utilisateurs.

QUE FAIRE ?
La première étape consiste à identifier :

- ☐ Si vous collectez des données à caractère personnel ? Sensibles ?
- ☐ Etes-vous responsable de traitement ou sous-traitant ?

LEXIQUE

Donnée personnelle : Information qui permet d'identifier **directement (nom) ou indirectement (n° de Sécurité Sociale, etc.)** une personne physique (les entreprises ne sont donc pas concernées).

Les données sensibles : Données liées à l'origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques, appartenance syndicale, données génétiques, données biométriques, données de santé,… **les données sensibles impliquent des obligations accrues et spécifiques.**

Le **responsable** du **traitement** de données personnelles : La personne, l'autorité publique, le service ou l'organisme qui détermine les finalités du traitement (à quoi il va servir) et ses moyens (selon quelles modalités).

Sous-traitant : Toute personne traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant.

FICHE N°1 : LES PRINCIPES A RESPECTER ET LES NOUVEAUX OUTILS DE CONFORMITE

COLLECTE LICITE

La collecte se fait licitement, avec le consentement de la personne concernée pour l'exécution d'un contrat, et **loyalement**, en faisant preuve de transparence. Les données doivent en principe être collectées directement auprès de la personne concernée et elle doit en être informée, y compris lors d'un transfert des données.

Les finalités du traitement doivent être déterminées dès l'origine. En cas d'évolution des finalités, il faudra informer de nouveau les personnes concernées et obtenir leur consentement.

PRINCIPES ELEMENTAIRES

Il faut également appliquer la **minimisation**, c'est-à-dire ne collecter que les données qui sont nécessaires et pertinentes.

Enfin, les données doivent être collectées pour une **durée raisonnable** et un **délai de conservation** fixé au préalable. Elles seront détruites lorsque ce délai arrivera à échéance.

Privacy by default : Le responsable de traitement doit garantir que, par défaut, seules les données nécessaires seront traitées et que ces données ne seront accessibles qu'à un nombre de personnes déterminé.

Privacy by design : La protection des données doit être prise en compte dès la conception des nouveaux produits, services et traitements, puis tout au long de la vie du traitement.

> **EN BREF**
> Les principes de loyauté, de transparence, de proportionnalité et de sécurité guident l'ensemble des obligations du RGPD (analyse des traitements, information des personnes, etc.).

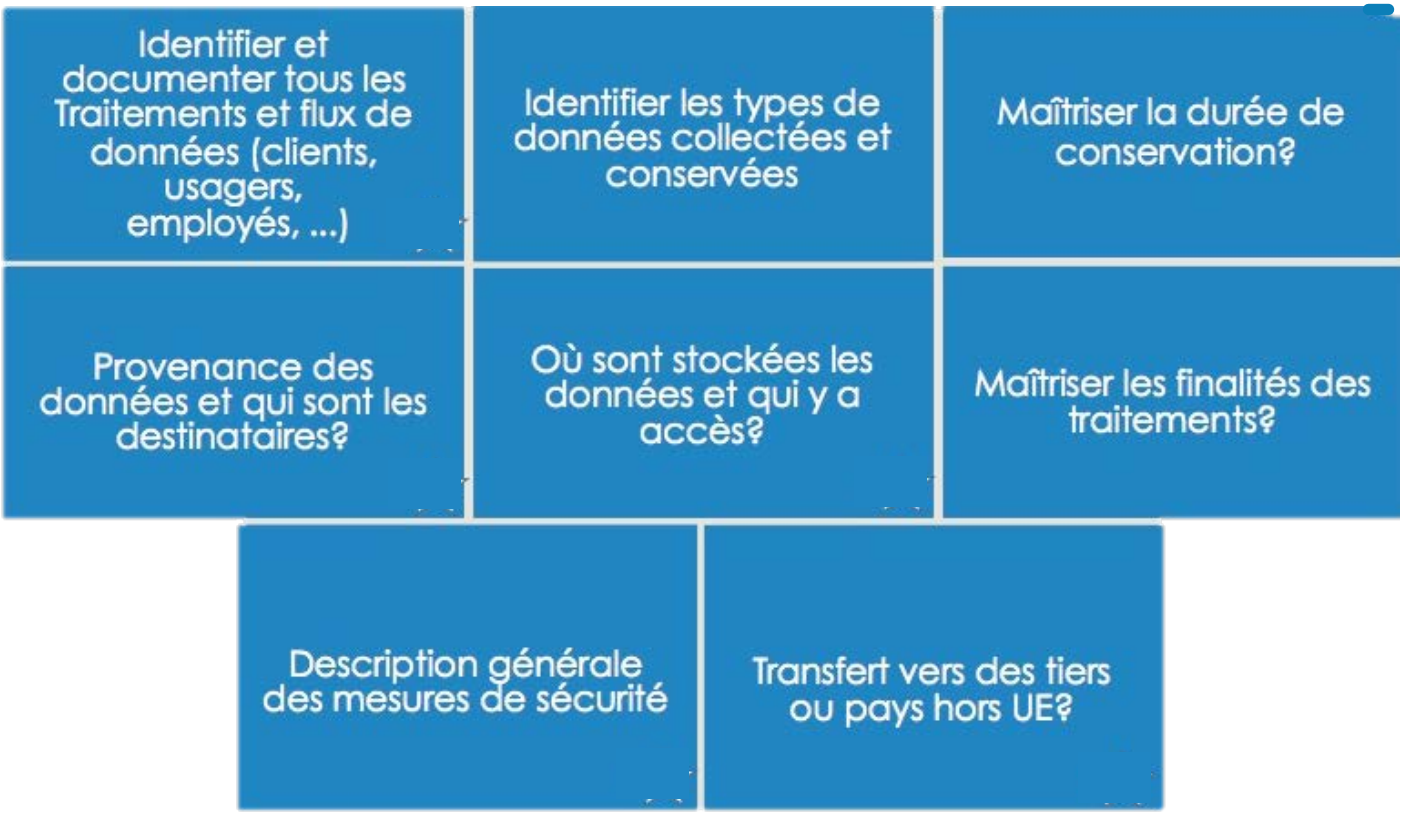
LES NOUVEAUX OUTILS DE CONFORMITE

Le registre des activités de traitement : Il recense les traitements, les catégories de données, les personnes concernées, les finalités, les destinataires, les délais, les mesures de sécurité, etc. Il est obligatoire pour les organismes de plus de 250 personnes.

L'analyse d'impact : Il faut construire un audit préalable à l'utilisation des données : description, évaluation du besoin, évaluation des risques, et mesures envisagées. Il est obligatoire si l'opération envisagée présente un risque élevé.

Le Délégué à la Protection des Données : Le DPO est obligatoire dans certains cas (organismes publics, suivi régulier et systématique à grande échelle, données sensibles). C'est le chef d'orchestre de la conformité. Il informe, conseille, contrôle et fait le lien avec l'autorité. Interne ou externe, il doit être indépendant et bénéficier des moyens suffisants pour accomplir sa mission.

LE REGISTRE DES ACTIVITES DE TRAITEMENT



FICHE N°2 : LA SECURITE DES DONNEES

« Les données doivent être traitées de façon à garantir leur sécurité y compris contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle.»

PSEUDONYMISATION

Une des mesures de confidentialité introduite par le RGPD est la **pseudonymisation** qui permet de ne plus identifier directement la personne (par le biais d'un code ou autre). Elle se distingue de l'anonymisation qui, elle, est irréversible.

ENVIRONNEMENT SECURISE

- Sécurité physique des locaux
- Anti-virus
- Modification périodique des mots de passe
- Protocole sécurisé en cas de transfert des données
- Recours au protocole HTTPS, etc.

SECURITE INFORMATIQUE

Les données doivent être l'objet d'obligations de **confidentialité**, des niveaux d'habilitation pour limiter l'accès aux données, une politique de sécurité informatique, etc.

CHOIX DES TIERS

La mise en sécurité des données recueillies passe également par le recours à des fournisseurs présentant des garanties suffisantes (voir page 4) et une évaluation régulière du niveau de sécurité.

EN BREF

Toutes les mesures de sécurité utiles doivent être mises en œuvre : votre imagination ne doit pas avoir de limite. La jurisprudence, en pratique, va quasiment jusqu'à imposer une obligation de résultat en la matière.

QUE FAIRE ?

Mettre en place et identifier les mesures de sécurité prises :

- ☐ En interne, vis-à-vis de vos collaborateurs
- ☐ En interne, sur vos systèmes informatiques
- ☐ En externe, lors du transfert des données
- ☐ En externe, avec vos fournisseurs et sous-traitants

FICHE N°3 : LES SOUS-TRAITANTS ET LES TRANSFERTS DE DONNEES

« Les sous-traitants doivent se conformer à des obligations concernant les données traitées pour leur propre compte mais aussi pour le compte de leurs clients. »

CONTRAT ENTRE RESPONSABLE DE TRAITEMENT ET SOUS-TRAITANT

Ce contrat doit contenir la description du traitement final des données et des devoirs du sous-traitant : Agir uniquement sur instruction du responsable de traitement et respecter l'intégralité des principes énoncés dans les fiches 1 et 2.

Les sous-traitants encourent les mêmes sanctions que les responsables de traitement.

LES TRANSFERTS DE DONNEES HORS UNION

Les transferts de données en dehors de l'Union européenne doivent présenter les garanties de protection suffisantes et ne sont autorisés que dans certains cas limités :

Transfert vers un pays reconnu pour son degré de protection des données (Suisse, Canada, Argentine, Nouvelle-Zélande, etc.)[1]

Mise en place de règles d'entreprises contraignantes (BCR) au sein des groupes, de clauses contractuelles types approuvées ou d'une certification.

BON A SAVOIR

Si le sous-traitant détermine les finalités et les moyens du traitement, il sera considéré comme co-responsable du traitement : prestataires, veillez à bien répartir les rôles et obligations de chacun dans le contrat conclu avec vos clients.

QUE FAIRE ?

Les responsables de traitement : identifier les transferts de données et signer des contrats de sous-traitance.

Les sous-traitants : proposer une solution respectueuse du RGPD avec la mise en place des outils exigés, véritable atout concurrentiel.

[1] Pour les Etats-Unis, le Privacy Shield a été adopté le 1er août 2016 pour les transferts aux entreprises adhérentes. La vigilance est toutefois recommandée compte tenu des inquiétudes manifestées par de nombreuses associations (dont le comité des « CNIL » européennes) et la politique du renseignement mise en place par la présidence actuelle.

FICHE N°4 : LES DROITS DES PERSONNES CONCERNEES

TRANSPARENCE

L'information de la collecte doit être donnée par écrit ou voie électronique, lors de la collecte mais aussi lorsque les données sont utilisées dans de nouvelles conditions.

Le consentement doit être libre, spécifique et transparent. Il doit pouvoir être révoqué à tout moment.

LES DROITS

Les droits d'accès et de rectification restent applicables.

La portabilité ajoute la possibilité de récupérer les données fournies dans un format structuré et lisible pour les transmettre éventuellement à un autre prestataire (changement de fournisseur de messagerie, de banque, etc.).

Droit à l'oubli - La personne concernée pourra obtenir l'effacement de ses données, sauf cas particuliers.

Droit à un recours - Toute personne a le droit à un recours auprès de la CNIL ou du juge.

LE PROFILAGE

La pratique du profilage est définie dans le RGPD et des dispositions spécifiques sont prévues : Une information renforcée auprès des personnes concernées pour indiquer que leurs données feront l'objet d'études spécifiques et de décisions en conséquences ainsi que le droit d'opposition à cette pratique.

BON A SAVOIR

Le RGPD a ajouté des dispositions sur le consentement des mineurs : pour certains services, le consentement d'un enfant de plus de 16 ans[2] sera valable. Pour les plus jeunes, le consentement de leurs parents est exigé et le responsable doit s'efforcer de vérifier sa réalité.

[2] Les Etats pourront abaisser cette limite jusqu'à 13 ans

FICHE N°5 : LES SANCTIONS DE LA CNIL

SANCTIONS ADMINISTRATIVES

Amendes « Chaque autorité de contrôle veille à ce que les amendes administratives(…) soient, dans chaque cas, effectives, proportionnées et **dissuasives**. »

Hier limitées à 150 000 euros, puis à 3 millions d'euros en 2016, les amendes pourront désormais atteindre **10 à 20 millions d'euros ou 2 à 4 % du chiffre d'affaires global mondial,** selon l'infraction constatée.

Injonctions : La CNIL peut également prononcer des injonctions, des mises en demeure, des limitations ou interdictions des traitements, ou des avertissements **publics**.

Sanctions pénales : Selon l'infraction, jusqu'à 5 ans d'emprisonnement et 300 000 euros d'amende pour le chef d'entreprise.

Sanctions civiles : Toute personne peut saisir le juge d'une demande de dommages-et-intérêts. Ce droit est désormais renforcé par la consécration des actions collectives.

En outre la CNIL, libérée des formalités de déclaration préalable, renforce ses rôles d'information, de conseil et de contrôle.

BON A SAVOIR

Toute violation de données doit être notifiée à l'autorité dans un délai de 72 heures. Les personnes concernées devront être informées « dans un délai raisonnable » si la faille de sécurité présente un « risque élevé » pour ses droits et libertés. Les délais imposés étant courts et la preuve de la conformité ne pouvant être réalisée a posteriori, il ne faut pas attendre un contrôle ou une action pour se mettre en conformité !

LES ETAPES A SUIVRE

MAINTENANT QUE VOUS AVEZ TOUTES LES INFORMATIONS NECESSAIRES, COMMENT VOUS METTRE EN CONFORMITE ?

1. DESIGNER UN PILOTE

Un chef d'orchestre qui éduquera et expliquera la règlementation en interne, coordonnera l'intervention, le rôle et les responsabilités de chaque département ou prestataire concerné, tant en interne, qu'en externe (conception, marketing, commerciaux, informatique, juridique…).
Dans l'objectif d'anticiper la désignation d'un DPO, qui pourra être un salarié ou un conseil externe, disposant des connaissances exigées sur la protection des données.

2. L'ETAT DES LIEUX

Un audit pour connaître vos obligations, il convient au préalable d'identifier tous les traitements de données réalisés et leur nature : catégories de données, modalités de collecte, de conservation, etc.
Dans l'objectif de préparer votre registre des activités de traitement.

3. LE DIAGNOSTIC

Une analyse pour connaître précisément vos obligations en fonction de leur nature (données sensibles, traitement à grande échelle, prestataires concernées…).
Dans l'objectif de préparer une roadmap identifiant et priorisant les actions à mener.

4. METTRE EN PLACE LES PROCEDURES

Adapter les traitements réalisés, modifier les mentions d'information, établir une politique de protection des données ou une charte numérique, sensibiliser les salariés, revoir les contrats avec les sous-traitants, faire une analyse d'impact…
Dans l'objectif de mettre en place toutes les procédures en interne qui guideront votre gestion des données personnelles.

5. CONSTITUER SON DOSSIER DE CONFORMITE

Dater et regrouper sa documentation, les politiques mises en place, les études d'impact, les contrats, le registre des activités de traitement, etc.
Dans l'objectif de faire valoir votre conformité auprès de vos clients, de vos concurrents, de vos partenaires et de transformer votre politique de protection des données en véritable atout concurrentiel.

PINT AVOCATS VOUS ACCOMPAGNE DANS VOTRE MISE EN CONFORMITE :

SENSIBILISATION (ATELIER D'UNE DEMI-JOURNEE)

Présentation du cadre légal
Sensibilisation de tout le personnel de votre entreprise : formation et acquisition des réflexes

DIAGNOSTIC (INVENTAIRE D'UNE JOURNEE - MEMO DE PRECONISATIONS PERSONNALISEES)

Réunion d'une journée et rencontre avec le DSI et les différents départements (DRH, marketing, comptabilité…)
Restitution dans les 60 jours d'un mémo d'analyse de vos obligations en fonction des traitements
Identification des actions à mener dans votre entreprise

MISE EN CONFORMITE (MISE EN PLACE DES OUTILS NECESSAIRES)

Rédaction des registres de traitement - Revue des contrats fournisseurs - DPO, étude d'impact, etc.
Et ½ journée de validation des bonnes pratiques mises en œuvre dans les 6 mois.

www.pint-avocats.fr

Avocats au Barreau de Marseille
Cabinet en Droit des Affaires et en Droit des Nouvelles Technologies,
de l'Informatique et de la Communication, Droit de la Propriété Intellectuelle

Athélia IV - Espace Mistral – Bât. A
297, avenue Mistral
13600 La Ciotat
Tel: +33 (0)4 42 700 703
Fax: +33 (0)4 42 83 51 07