RGPD

La protection des données personnelles est un droit fondamental consacré à la fois par l'article 8 de la Charte des droits fondamentaux de l'UE et par l'article 16 du Traité Sur le fonctionnement de l'UE (TFUE) (✓"*Toute personne a droit à la protection des données à caractère personnel la concernant*".)

▶Le RGPD (ou GDPR) est le règlement européen sur la protection des données. Il est entré en application en **2018** et impacte toutes les entreprises opérant du traitement de données à caractère personnel sur des résidents européens.

Objectifs:

- Uniformiser au niveau européen la réglementation sur la protection des données.
- Responsabiliser davantage les entreprises en développant l'auto-contrôle.
- Renforcer le droit des personnes (droit à l'accès, droit à l'oubli, droit à la portabilité, etc.).

—->Les règles duRGPD s'appliquent à toutes les entreprises privées ou publiques des 27 Etats membres de l'Union européenne. Plus précisément, aux entreprises :

- Proposant des biens et services sur le marché de l'UE.
- Collectant et traitant des données à caractère personnel sur les résidents de l'UE.

⚠ ⚠ A noter que le règlement s'applique aussi aux entreprises non implantées en UE , **dès lors qu'elles collectent et traitent des données personnelles sur des résidents de l'UE.** Autrement, le règlement s'applique donc à chaque fois qu'un résident européen, quelle que soit sa nationalité, est directement visé par un traitement de données, y compris par internet ou par le biais d'objets connectés (comme les appareils domotiques, les objets mesurant l'activité physique, etc.).

➡ ➡ Les règles et obligations du RGPD s'appliquent au traitement - automatisé ou non des pratiques en matière de collecte et d'utilisation des données à caractère personnel.

Le RGPD donne une définition précise des « données à caractère personnel » : il s'agit de « **toute information se rapportant à une personne physique identifiée (nom/prénom/numéro..) ou identifiable (**)».Le RGPD concerne uniquement la protection des données personnelles **rattachées à des personnes physiques.**⚠ Ce qui signifie que le RGPD ne s'applique pas aux entreprises ne traitant que des données relatives à des personnes morales**, sauf si celles-ci sont amenées à collecter des données sur des représentants des personnes morales**. En revanche, la collecte d'informations sur l'entreprise (dénomination sociale, objet social, ...) en est exclue.

Le « traitement des données », au sens de **l'art. 4 du RGPD**, fait référence à la **collecte, à l'accès, au stockage, à la manipulation, à la destruction et à la consultation à distance des données.▶ pas nécessairement informatisé**

PRINCIPES

- Les données personnelles doivent être "traitées de manière licite, loyale et transparente" et "collectées pour des finalités déterminées, explicites et légitimes".
- Elles doivent être "adéquates, pertinentes et limitées" aux finalités du traitement, être "exactes et, si nécessaire, tenues à jour".
- Elles doivent être conservées de façon réduite dans le temps et dans des conditions de "sécurité appropriée".

✓C'est ainsi que les dispositions du GDPR s'articulent autour de 4 principes clés : **le consentement, le droit des personnes, la transparence et la responsabilité.**

Le consentement

Il doit être explicite et « positif » (interdiction notamment des cases pré-cochées). Ce consentement peut être retiré à tout moment par les individus le demandant. Les entreprises faisant du traitement de données doivent, par ailleurs, être en mesure de prouver le recueil de ce consentement (en cas de contrôle de la CNIL).

⚠ Le consentement des enfants est pour la première fois encadré. **Le RGDP fixe à 16 ans l'âge à partir duquel un mineur peut consentir seul au traitement de ses données personnelles pour utiliser un service sur internet, typiquement les réseaux sociaux.** En deçà de 16 ans, l'autorisation des parents est nécessaire.

⚠ En outre, le traitement des données personnelles dites sensibles (*des données relatives à l'origine raciale ou ethnique, aux opinions politiques, aux convictions religieuses ou philosophiques, à l'appartenance syndicale…*) est interdite sauf dans des cas limitatifs et sous conditions.

⚠ RGPD emporte aussi des conséquences dans le mode de gestion des cookies. La nouvelle réglementation impose la mention des infos suivantes : ☑ la finalité du cookie, ☑ le droit d'opposition de l'utilisateur et☑ l'acceptation implicite de l'utilisateur si celui-ci décide de poursuivre sa navigation. Le bandeau d'information ne doit pas disparaître tant que l'utilisateur n'a pas poursuivi sa navigation.

✓*Remarque*: Les cookies donnent des informations sur les préférences de la personne qui visite le site. Les cookies sont aussi utiles pour obtenir des statistiques sur le site web en question : temps de consultation des pages.
Autre conséquence : **désormais, aucun cookie ne peut être déposé si l'utilisateur rebondit sur la page - sauf les cookies nécessaires au bon fonctionnement du site.**

⚠ Autre évolution majeure : **l'encadrement du profilage.** Le RGDP définit le profilage comme « *toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les*

déplacements de cette personne physique ». Le règlement renforce son encadrement. Il impose notamment **le recueil d'un consentement explicite de la part des personnes (case à cocher).** Le profilage est désormais soumis au droit d'opposition.Le responsable de traitement doit également fournir des informations utiles concernant la logique sous-jacente de l'algorithme, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée. **L'article 22** prévoit le droit de la personne concernée d'obtenir une intervention humaine de la part du responsable du traitement, d'exprimer son point de vue et de contester la décision. Le profilage n'est pas autorisé en matière de données « sensibles ».

La transparence

▶Il s'articule au consentement, dans la mesure où **la transparence est la condition de possibilité d'un consentement éclairé et explicite**. Les e/ses sont tenues, dès la phase de collecte ,de fournir aux individus des informations claires et sans ambiguïté sur la manière dont leurs données seront traitées. Ces infos doivent être fournies de façon **concise**, **compréhensive** et **accessible** par tous.

Le droit des personnes

—>Un des principaux objt du GDPR est de renforcer les droits des personnes physiques.
Dans ce cadre,les résidents européens se sont vu attribuer de nouveaux droits :

- **Un droit d'accès facilité pour tous les utilisateurs.** Le responsable du traitement doit faciliter l'exercice de ce droit, par la mise en place de process et d'outils adaptés. En cas de demande d'accès de la part d'un utilisateur, l'entreprise dispose d'un **délai maximum d'un mois** pour la satisfaire.
- **Un droit l'oubli pour tous les utilisateurs.** Les entreprises dispose **d'un délai réduit d'un mois, et non plus de deux mois,** pour supprimer les données à la suite d'une demande. (copies + reproductions des données)
- **Un droit à la limitation du traitement, applicable** dans quelques cas précis.
- **Un droit à la portabilité des données.** Ce droit permet à une personne de récupérer les données qu'elle a fournies, sous une forme aisément réutilisable et, le cas échéant, de les transférer à un tiers.
- **Action de groupe** : toute personne peut mandater une association ou un organisme actif dans le domaine de la protection des données pour introduire une réclamation ou un recours et obtenir réparation en cas de violation de ses données;
- **Droit à réparation du dommage matériel ou moral** : toute personne qui a subi un tel dommage du fait de la violation du RGPD peut obtenir du responsable du traitement ou du sous-traitant la réparation de son préjudice.

La responsabilité (accountability)

➡ Responsabiliser les e/ses.

- **L'obligation faite aux entreprises de documenter toutes les mesures et procédures en matière de sécurité des DCP.** ▶l'obligation de tenue d'un registre des traitements.
- **Le renforcement des mesures de sécurité.** (*pseudonymisation des données, analyses d'impact, tests d'intrusion*...).
- **La mise en avant du principe de « Privacy By Design ».** Les entreprises doivent prendre toutes les mesures permettant de protéger les droits des personnes en amont (-dès la conception d'un produit ou d'un service) et tout au long du cycle de vie des données (de leur collecte à leur suppression).
- L'encadrement des sous-traitants insertion de clauses... **En cas de faille de sécurité au niveau du sous-traitant, ce sera l'entreprise cliente (= le responsable des traitements) qui sera tenue pour responsable.** (➡ *co-responsabilité des sous-traitants*).
- **La notification en cas de faille de sécurité** (*data breach*). Les entreprises ont pour obligation de mettre en place des actions en cas de violation de sécurité⚠ ⚠ ⚠ En cas de faille de sécurité, l'entreprise doit la notifier à l'autorité de régulation compétente (En France, la *CNIL*) **dans un délai de 72h. Les personnes concernées doivent être informées « dans les meilleurs délais »** si la faille ou la violation de données comporte un risque élevé pour les droits et libertés.
- **L'obligation de désignation d'un Data Protection Officer**; chargé de piloter la gouvernance des données, de contrôler la conformité de l'entreprise avee le GDPR et de conseiller le responsable des traitements. (⚠ *pour les eses réalisant des traitements sur des données sensibles et/ou à grande échelle.*)
- La suppression de l'obligation de déclaration préalable à la CNIL. Cette mesure traduit le principe qui gouverne le RGPD : responsabiliser les entreprises, en développant l'auto-contrôle.

—-EN CAS DE NON RESPECT :

Multiplicité des actions en justice en cas d'atteinte aux données personnelles ;

- Recours RGPD devant la Commission nationale informatique et libertés (Cnil) : **(ART 77 du RGPD)**

La personne concernée peut effectuer un recours RGPD devant l'autorité de contrôle de:
—>l'État membre dans lequel se trouve sa résidence habituelle;
—->son lieu de travail;
——>le lieu où la violation aurait été commise.
Ou aussi en mandatant un organisme, une organisation ou une association à but non lucratif, dont les objectifs statutaires doivent être d'intérêt public, et qui doit être actif dans le domaine de la protection des droits et , des libertés des personnes concernées.

- Engager une action devant les tribunaux contre la décision de la Cnil (article 78 du RGPD)

Et ce lorsque :
- Non satisfaction de la décision juridiquement contraignante rendue par l'autorité de contrôle;
- Non obtention, **dans un délai de 3 MOIS**, aucune réponse ni d'information de l'état d'avancement de son recours de la part de l'autorité de contrôle.

➡ Le recours doit être fait devant le juge de l'État membre où l'autorité de contrôle a son siège.

- Engager une action au pénal contre le responsable du traitement ou un sous-traitant

Ainsi si la personne concernée pourra obtenir réparation en effectuant un recours devant les juridictions de;

l'État membre dans lequel la personne concernée a sa résidence habituelle, sauf si le responsable du traitement est une autorité publique d'un État membre agissant dans l'exercice de ses prérogatives de puissance publique.

devant les juridictions de l'Etat dans lequel le responsable du traitement ou le sous-traitant dispose d'un établissement.

CO RESPONSABILITÉ _ *Le responsable du traitement est en principe le premier responsable, mais le sous-traitant peut être solidaire, voire se faire imputer de toute la responsabilité. Toutefois, une exonération est possible s'ils arrivent, chacun, à démontrer que cela ne leur est pas imputable.*

SANCTIONS?

✓**Toutes les entreprises traitant des données sont concernées par les sanctions RGPD**. Dès lors qu'une entreprise traite des données, elle doit respecter de nombreuses obligations prévues par le RGPD.

Les sanctions pénales (1) et administratives (2) (versées au TRÉSOR PUBLIC,pas DE D&I)

->La **CNIL** est l'autorité en charge du respect des obligations prévues par le RGPD en France. A ce titre, elle ne manque pas de sanctionner les responsables de traitement et sous-traitants n'exécutant pas leurs obligations.

(1);

- En cas de non-respect de l'obligation d'information des personnes, l'entreprise s'expose à une amende de 1 500€ pour chaque infraction.
- Non-respect des droits des personnes = une amende de 1 500€ pour chaque infraction.
- Détournement de la finalité des données personnelles =5 ans d'emprisonnement et 300 000 € d'amende.
- Risque d'atteinte à la réputation de l'entreprise➡ Diffusion par la CNIL d'un document officiel détaillant le manquement et le montant de l'amende.

(2):

- Jusqu'à **10** millions d'euros ou 2% du chiffre d'affaires mondial pour des manquements relatifs à la mise en conformité.
- Jusqu'à **20** millions d'euros ou 4% du chiffre d'affaires mondial pour des manquements relatifs aux droits des personnes.