Partie I: Présentation générale du Règlement européen

Entrée en vigueur et champs d'application territorial

- **Entrée en vigueur**

- **Champs d'application territorial du Règlement**
  - Union Européenne : en fonction du **lieu d'établissement de l'entité**

  S'applique aux traitements de données à caractère personnel effectués par un responsable de traitement ou un sous-traitant établi sur le territoire de l'UE.

  - Hors Union Européenne :

  → S'applique si les personnes concernées sont sur le **territoire d'un Etat membre**.

  → ex : entreprise établie aux USA qui commercialise ses produits directement en France, sans être présente sur le territoire de l'UE = soumise aux exigences du RGPD.

Points clés *: Collecte de données à caractère personnel (1)*

× Données à caractère personnel

→ « ***toute information se rapportant à une personne physique identifiée ou identifiable*** *» (personnes concernées)*

- Données permettant l'identification directe :

nom, prénom, …

- Autres données : *numéro de sécurité*

sociale, adresse IP, données de localisation,

identifiant du salarié au sein de l'entreprise, …

× Traitement

→ ***Opération*** *(ou ensemble d'opérations)* ***effectuée****(s)* ***ou non à l'aide de procédés automatisés*** *et* ***appliqués à des données à caractère personnel***

Ex. *collecte, enregistrement, conservation , diffusion = traitements*

Points clés *: Collecte de données à caractère personnel (2)*

× **Licéité de la collecte** – inchangée avec le RGPD

→ Conditions **cumulatives** :

- Loyauté et licéité
- Finalité déterminée, explicite et légitime
- Pertinence et proportionnalité des données
- Conservation limitée
- Sécurisation des données

- *Quid des traitements non automatisés* ?

Si les données sont contenues dans un ensemble structuré de données accessibles selon des critères déterminés = collecte de données.

Points clés *: Responsable de traitement et sous-traitance (1)*

- **Le Responsable de traitement**

Obligations renforcées par le Règlement.

→ *Personne physique ou morale, l'autorité publique, qui seul ou conjointement avec d'autres,* ***détermine les finalités, les moyens de traitement.***

= le responsable de traitement met en œuvre le traitement dans son intérêt, en son nom et pour son propre compte.

Responsables « **conjoints** » : définir de manière transparentes les obligations respectives de chacun.

Points clés *: Responsable de traitement et sous-traitance (2)*

- **Le sous-traitant : personne physique ou morale qui traite des données à caractère personnel pour le compte du responsable du traitement (ex prestataires paie)**

Rééquilibre des relations entre responsable de traitement et sous-traitant.

- S'assurer de la **fiabilité du sous-traitant**
- **Contrat de sous-traitance** : *comportant notamment l'objet, la durée, la nature, la finalité du traitement, également le type de données à caractère personnel, les catégories de personnes concernées, les droits et obligations du responsable de traitement*.

→ seul le responsable de traitement donne instruction de traiter des données à caractère personnel

→ le sous-traitant devra s'assurer de la confidentialité des données, et prendre des mesures à cet effet

→ Information immédiate du responsable de traitement en cas de violation des données à caractère personnel

= responsabilité du sous-traitant à défaut du respect des obligations du Règlement et/ou des instructions du responsable de traitement.

Les droits des personnes concernées (1)

- **Droits préexistants mais renforcé**
  - **Droit à l'information** : lorsque des données sont collectées, le responsable de traitement doit communiquer à la personne concernée certaines informations (*l'objectif de la collecte, les coordonnées du responsable de traitement, la durée de conservation des données, transfert éventuel …)*
  - **Droit d'accès/de rectification/à l'effacement** : demande auprès du responsable de traitement des informations à caractère personnel en sa possession. Le droit d'accès permet de contrôler l'exactitude des données, et au besoin de les faire rectifier, ou de les effacer (droit à l'oubli).
  - **Droit d'opposition** à un traitement des données personnelles sous certaines conditions : droit de s'opposer à figurer dans un fichier, à ce que les données soient diffusées, transmises ou conservées (*prospection commerciale)*. Droit de retirer son consentement (lorsqu'il avait été donné) à tout moment, sans porter atteinte à la licéité du traitement avant le retrait du consentement.
  - **Droit d'introduire une réclamation auprès d'une autorité de contrôle**
  - **Droit d'être informé d'une violation des données personnelles**

Les droits des personnes concernées (2)

- **Droit à la portabilité**

Droit de récupérer les données fournies dans un format structuré et lisible par machine auprès du responsable de traitement.

- Pour un usage personnel

- Pour un transfert d'un organisme à un autre

→ Facilite le partage de données personnelles de manière sécurisée, sous le contrôle de la personne concernée.

- **Droit à la limitation du traitement**

Dans des cas spécifiques. Par exemple, lorsque la personne concernée a exercé son droit d'opposition. Le traitement sera limité en attendant de savoir si les droits de la personne concernée prévalent sur les motifs légitimes poursuivis par le responsable de traitement.

La limitation entraîne le gel temporaire des données qui ne peuvent plus faire l'objet d'opérations de traitement ni être modifiées.

Les droits des personnes concernées (3)

/! Nouveau délai **d'un mois** (deux mois auparavant) à compter de la réception de la demande de la personne concernée pour y faire droit (droit à l'accès, à la rectification ou à l'effacement)

→ Ceci implique pour l'entreprise de s'adapter et d'être en mesure de répondre à d'éventuelle demande de la personne concernée. (par exemple procédure de gestion et de traitement des demandes d'exercice de leurs droits par les personnes concernées)

Un nouvel acteur : le Data Protection Officer – DPO (1)

Ancien Correspondant Informatique et Libertés (CIL), autrefois facultatif.

- DPO **obligatoires** dans **3 cas** :
  - Traitement effectué par une autorité/organisme public
  - Activité qui, par leur nature, leur portée, ou leur finalité, exigent un **suivi régulier** et à **grande échelle des personnes concernées**
  - Activité consistant en un **traitement à grande échelle de catégories particulières de données** (*condamnations pénales, données de santé, …)*

/! Même si ce n'est pas une obligation pour tous, le DPO à un rôle clé dans la mise en conformité des entreprises.

→ En pratique, il est chargé de **mettre en place une organisation fonctionnelle** dans l'entreprise autour d'acteurs confrontés directement à la conformité (*audit et risques, directions* juridiques, …).

Un nouvel acteur : le Data Protection Officer – DPO (2)

- **Désignation**
  - En interne
  - En externe (*contrat de prestation de service*)
  - Mutualisé : pour les groupes d'entreprise, le DPO organisera pour l'ensemble du groupe la conformité, les contrôles et la supervision des procédures.

- **Missions**
  - **Informer et conseiller** le responsable de traitement ou le sous-traitant, et les employés
  - **Contrôler le respect du règlement** et du droit national sur la protection des données,
  - **Conseiller l'organisme** sur la réalisation d'étude d'impact sur la protection des données, et en vérifier l'exécution
  - **Coopérer avec les autorités de contrôle**

Selon la CNIL, il devra donc être informé sur le contenu des nouvelles obligations. Il devra être en mesure de sensibiliser les décideurs sur l'impact de ces nouvelles règles. Le DPO participera à l'élaboration de l'inventaire des traitements de données, lui permettant de concevoir des actions de sensibilisation. Il aura pour rôle de piloter la conformité de manière continue.

Les nouvelles obligations des entreprises

→ **Responsabilisation et transparence, démarche proactive : passage d'un système déclaratif à une démarche proactive (« accountability »)**

→ Elle doit **être en mesure de prouver à tout moment l'efficacité des systèmes mis en place :**

En pratique, l'entreprise met en place de nouveaux procédés et procède à une organisation spécifique qui vont garantir la protection maximale des données faisant l'objet d'un traitement

2 nouveaux concepts :

- **Privacy by design**

= protection de la vie privée dès la conception.

→ Dès la conception d'un nouveau procédé, la confidentialité et la sécurité des donnes doivent être en place.

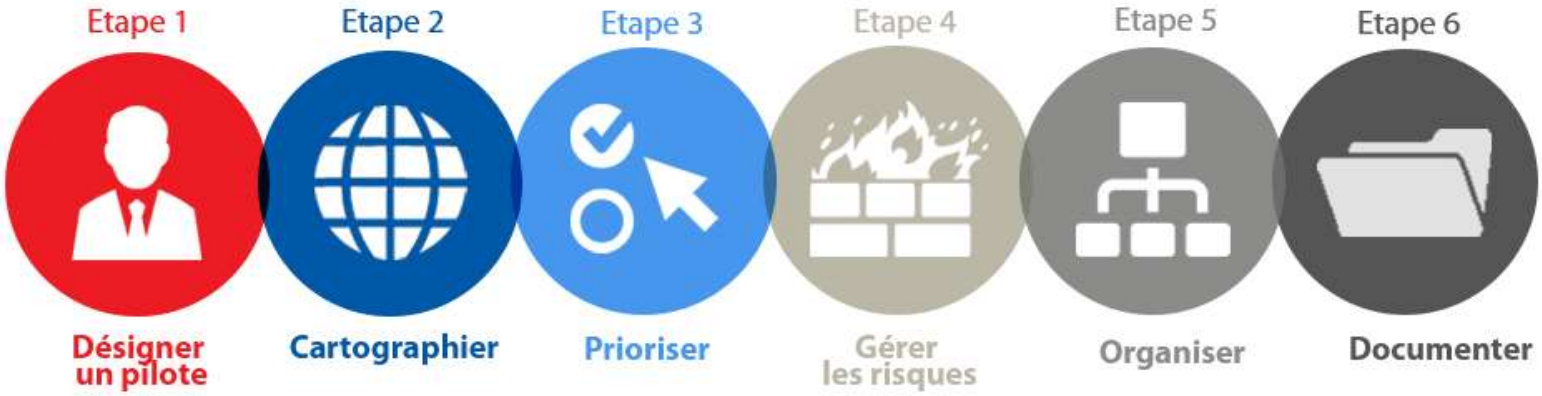
- **Privacy by default**

= protection de la vie privée par défaut.

→ seules les données à caractère personnel nécessaires au regard de la finalité d'un traitement seront collectées.

Partie II: La mise en conformité des entreprises

Les préconisations de la CNIL (1)



Focus sur le traitement des données des Ressources Humaines

<u>Etape 1</u> : *Cartographier (faire un état des lieux de ce qui est collecté et traité) et tenir un registre de traitement*

- *<u>Quelles données sont traitées</u> ?*

→**Avant le 25 mai,** Loi Informatique et Libertés : déclaration auprès de la CNIL

Ex. *Norme simplifiée n°46 qui concerne la gestion des RH, n°42 sur les badges dans les lieux de travail, AU-004 pour les dispositifs d'alerte professionnelle, dispense DI-002 relative à la paie des personnels du secteur privé.*

→ **Après le 25 mai**, RGPD : processus simplifié

Le RGPD allège grandement les formalités mais introduit en contrepartie de nouvelles obligations pour le responsable de traitement. Pour les entreprises **de + de 250 salariés**, obligation de tenir un registre des traitements mis à disposition de la CNIL (doit contenir des informations supplémentaires telles que le transfert des données vers un pays tiers).

/! La tenue de ce registre est parfois conseillé pour les entreprises de – 250 salariés

L'entreprise devient elle-même **actrice de sa mise en conformité**. Elle fera **sa propre évaluation de conformité** entre le traitement envisagé et les exigences liées à la règlementation européennes et nationales. Elle devra être en mesure de **justifier sa conformité** à tout moment et par le biais d'une **documentation fournie et à jour**.

Focus sur le traitement des données des Ressources Humaines

Cartographier = consiste à comprendre quel type de données sont détenues par votre entreprise : qui en a la responsabilité, d'où elle proviennent, avec qui elles sont partagées, comment elles sont utilisées, à quelles fins elles sont collectées, où elles sont stockées.

Peut se faire manuellement. Lorsque l'entreprise brasse davantage de données = conseiller d'envisager d'investir dans des outils informatiques (dont la tenue du registre de traitement).

La CNIL préconise donc de se poser les questions suivantes :

- Qui ?
- Quoi ?
- Pourquoi ?
- Jusqu'à quand ?
- Comment ?

Focus sur le traitement des données des Ressources Humaines

Ex. *de cartographie des traitements relatifs aux Ressources Humaines.*

Recrutement	→ **Entretiens avec les candidats** *CV, lettre de motivation* **/!** La CNIL considère que la collecte du numéro de sécurité sociale n'est pas nécessaire lors du recrutement
Exécution du contrat de travail	→ **Evaluation annuelle des salariés** *Date des entretiens, compétences professionnelles, objectifs et résultats, évolution de carrière* → **Contrôle de l'activité du salarié** → **Gestion des outils/matériels mis à disposition du salarié** *Véhicule, téléphone, ordinateur*
Santé et sécurité au travail	→ **Dispositifs mis en place liés à la santé et la sécurité au travail** *Système de vidéosurveillance, système de badges*
Service comptable	→ **Gestion comptable** *Bulletins de paie incluant les éventuels avantages en nature des salariés ; gestion des tickets-restaurants*
Relations avec les Instances Représentatives du Personnel (IRP)	→ **Syndicat** *Election des délégués syndicaux* → **Comité social et économique** (ancien CE) *Gestion des activités sociales et culturelles mis en place par l'employeur*
Prestataires extérieurs sous-traitant des données personnelles	→ **Mise à jour des contrats conclus avec des sous-traitants** *Prestataires extérieurs notamment la paie*

Focus sur le traitement des données des Ressources Humaines

<u>Etape 2</u> : *Minimisation des données et durée de conservation*

- Ne collecter que les **données adéquates, pertinentes et limitée à ce qui est strictement nécessaires à la finalité de traitement**

Ex. dans le cas d'un recrutement, les données ne doivent servir qu'à évaluer la capacité du candidat à occuper l'emploi proposé.

→ seules les données relatives à la qualification et aux expériences professionnelles du candidat sont nécessaires la finalité de traitement et peuvent être collectées (diplômes, emplois précédents etc...)

→ il est donc interdit de demander à un candidat son numéro de sécurité sociale, de collecter des données sur la famille du candidat, de collecter des données sur les opinions politiques ou l'appartenance syndicale du candidat.

Focus sur le traitement des données des Ressources Humaines

- *Limitation des finalités de traitement*

Les données personnelles sont collectées pour des finalités **déterminées, explicites et légitimes**, et ne peuvent être traitées ultérieurement de manière incompatible avec ces finalités.

Chaque traitement nécessite de « *préserver la* ***protection à la dignité humaines****, les* ***intérêts légitimes*** *et* ***les droits fondamentaux des personnes concernées […]*** » **-** (RGPD, art. 88 sur le traitement des données dans le cadre des relations de travail).

Focus sur le traitement des données des Ressources Humaines

- **Gestion administrative du personnel**

  L'employeur peut collecter principalement deux types de données :
  • des données nécessaires au respect d'une obligation légale
  • des données utiles à la gestion administrative du personnel, à l'organisation du travail et à l'action sociale.

- **Contrôle de l'activité du personnel**

  L'employeur peut mettre en place différents outils afin de contrôler l'activité du personnel.

  Par exemple, l'employeur pourrait encadrer les conditions d'utilisation d'Internet par le personnel sur leur lieu de travail. Il peut mettre en place des filtres afin de bloquer certains contenues (pornographie, pédophilie, etc.). Il est également possible de limiter l'utilisation d'Internet pour des raisons de sécurité par exemple le téléchargement de logiciels, la connexion à un forum, etc.

- **Gestion et contrôle de l'accès aux locaux**

  Mise en place des dispositifs afin de contrôler les horaires et l'accès du personnel.

Focus sur le traitement des données des Ressources Humaines

- **Interdiction de traitement des données sensibles** sauf dérogations particulières spécifiquement prévue .

Quelques exemples :

→ origine raciale ou ethnique
→ opinions politiques
→ convictions religieuses ou philosophiques
→ données génétiques
→ données concernant la santé

Focus sur le traitement des données des Ressources Humaines

- **Bien définir la finalité du traitement des données**

→ une Jurisprudence s'est développée ces dernières années : le salarié licencié pour faute utilise un manquement de son employeur à l'une de ses obligations lui incombant en matière de conformité « Informatique et Liberté ».

→ ex. le dispositif n'a pas fait l'objet d'une déclaration préalable à CNIL et par conséquent, le moyen de preuve n'est pas recevable.

→ ex. le salarié invoque une finalité illégitime (la finalité déclarée – se prémunir contre le vol - n'est pas celle qui a été utilisée – contrôle du salarié - pour justifier la sanction disciplinaire du salarié).

/!\ Risque qui sera d'autant plus important avec l'obligation de compliance qui pèse désormais sur l'entreprise. L'employeur n'ayant plus de déclarations préalables à adresser à la CNIL devra bien définir la finalité du traitement des données.

Focus sur le traitement des données des Ressources Humaines

- **Durée de conservation** des données personnelles

Elle doit être définie par l'entreprise.

→ Lorsque l'objectif du traitement est atteint, les données doivent être supprimées. Généralement, les données relatives au personnel sont conservées le temps de leur présence dans l'entreprise augmentées des durées de prescriptions légales. Après elles doivent être effacées ou anonymisés (pour par exemple les statistiques).

Ex. en cas de recrutement : *les CV et lettre de motivations des candidats non retenus doivent être supprimés rapidement sauf s'ils ont donné leur consentement.*

Focus sur le traitement des données des Ressources Humaines

<u>Etape 3</u> : *Information et Consentement des salariés et candidats*

- **Avertir sur la mise en place d'un traitement au moment où les données sont collectées**

Le responsable de traitement est **tenu d'informer** les salariés et candidats de l'entreprise de la **mise en place d'un traitement** des données, mais également **des finalités** et **des modalités** de ce traitement.

D'autres informations doivent être portée à la connaissance des personnes concernées, notamment : *la durée de conservation des données, les droits dont dispose la personne concernée, transferts des données, … .* (*)

Ces informations peuvent figurer sur le contrat de travail ou en pièce jointe, dans le règlement intérieur, faire l'objet d'un affichage ou d'une communication par courriel, notamment pour régulariser la situation auprès du personnel qui n'a pas été correctement informé. Le site internet de l'entreprise dès lors qu'il y a un formulaire à remplir (ex candidature en ligne)

- **Consentement de la personne concernée**

Selon le RGPD, il s'agit d'un **acte positif**.

La preuve de consentement est **à la charge du responsable de traitement**.

L'entreprise devra donc être en mesure de recueillir le consentement de manière certaine *(autorisation écrite, case à cocher, …)* et **/!** au *droit de retrait, au droit d'accès.*

Focus sur le traitement des données des Ressources Humaines

- ***(*) Les salariés doivent être informés***

• De l'identité et des coordonnées du responsable de traitement ;
• Des coordonnées du délégué à la protection des données lorsqu'il y en a un ;
• De l'objectif poursuivi (gestion administrative du personnel et du recrutement) ;
• De la base juridique du traitement ;
• De l'intérêt légitime s'il s'agit de la base légale du traitement ;
• Des destinataires des données (des sous-traitants de la gestion de paie, etc.) ;
• Des flux transfrontières ;
• De la durée de conservation ;
• Des conditions d'exercice de leurs droits d'opposition, d'accès, de rectification et de limitation, etc. ;
• Du droit de retirer son consentement s'il s'agit de la base légale du traitement ;
• Du droit d'introduire une réclamation auprès d'une autorité de contrôle ;
• Des informations sur le caractère réglementaire ou contractuel du traitement lorsqu'il s'agit de la base légale du traitement.

Focus sur le traitement des données des Ressources Humaines

<u>Etape 4</u> : *Garantir la sécurité et la confidentialité des données*

→ En coordination avec le DPO.

- **Mesures organisationnelles**

Gouvernance d'entreprise par la mise en place d'une **documentation interne** pour instaurer une culture d'entreprise et éviter toute divulgation à un tiers non autorisé.

Ex. *sensibiliser aux cyber-attaques et programmes malveillants.*

- **Mesures techniques**

Procédés physiques et informatiques permettant la sécurisation des données

Ex. *politique de gestion des incidents, sécurité des systèmes d'information, accès aux locaux.*

/! vérifier aussi les contrats entre responsable de traitement et sous-traitants (*prestataires de paies, …).*

Partie III : Les sanctions en l'absence de conformité

Violation des données personnelles (1)

- **Avertir la CNIL**
  - En cas de **violation susceptible d'entrainer un risque** pour les droits et libertés des personnes concernées

  Toute failles de sécurité entrainant destructions, perte, altération, révélation, accès non autorisé à ces données.

  - **Obligation de notification** (aujourd'hui seuls les fournisseurs de services de communications électroniques y sont soumis)

  - **Délai de 72 h maximum** à compter de la prise de connaissance des évènements.

  - **Information des personnes concernées** s'il y a un risque élevé pour leurs droits et libertés.

Violation des données personnelles (II)

× **Prévention d'une faille de sécurité**

→ Obligation de vigilance accrue

Mise en place de **mesures techniques et organisationnelles** pour **garantir un niveau de sécurité satisfaisant**.

En pratique, *comment répondre à cette obligation* ?

- Politique de sécurité spécifique à la protection des données personnelles
- Vérification et amélioration régulière de la politique de sécurité déjà existante
- Mise en place d'une procédure de gestion des failles de sécurité

Quelles sanctions en cas de non-conformité ?

× Amendes administratives

La sanction sera prononcée en fonction de la **nature,** la **gravité**, la **durée de l'infraction**, de la commission délibérée ou par négligence de l'infraction.

Le plafond prévu est très élevé.

- Jusqu'à **4% du chiffre d'affaire annuel mondial**
- **20.000.000 €**

→ le montant le plus élevé sera retenu

× Dommages et intérêts

Indemnisation de toutes personnes ayant subi un dommage du fait de la violation du règlement par le responsable de traitement.

× Sanctions pénales

Infraction spécifique en droit français : l'atteinte aux droits de la personne résultant de traitements informatiques

- Peine d'emprisonnement jusqu'à 5 ans
- Amende : 300.000 € pour les personnes physiques
  1.500.000 € pour les personnes morales