CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

PROTÉGER les données personnelles
ACCOMPAGNER l'innovation
PRÉSERVER les libertés individuelles

Panorama du Règlement Général sur la Protection des données personnelles

Formation CNEJITA – 20 juin 2017

Les 4 grands axes du RGPD

1. **Affirmation de la maîtrise des personnes sur leurs propres données**

   ✓ Droit à la portabilité, droit à l'oubli, droit d'opposition, transparence accrue

2. **Responsabilisation des organismes (du privé comme du public)**

   ✓ Désignation d'un Délégué à la Protection des données, documentation de chaque traitement, intégration de la protection de la vie privée par défaut et dès la conception, notification des failles de sécurité, contrôle des sous-traitants, etc.

3. **Pouvoirs de sanction accrus** : passe de 300 000 euros à 10 Millions d'euros (ou 2 % du CA) voire 20 Millions d'euros (ou 4% du CA)

4. **Renforcement de l'Europe face au GAFAM**

   ✓ Application si le traitement cible des européens ou les profile

   ✓ Coopération renforcée entre autorités européenne :

Panorama du RGPD

1. Un champ d'application étendu
2. "Responsabilisation" de nouveaux acteurs
3. Le renforcement du principe de licéité du traitement
4. Renforcement global des droits
5. L'accountability à l'heure du règlement
6. L'approche par les risques
7. Le délégué à la protection des données
8. La compétence étendue des CNILs

1 - Un nouveau champ d'application

Le règlement s'applique « ***au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier*** »

En revanche, il ne sera pas appliqué aux traitements mis en œuvre par :

- ✓ les institutions, organes et agences de l'Union européenne (règlement CE n° 45/2001)
- ✓ les Etats membres dans le cadre de la politique étrangère et de la sécurité commune
- ✓ les personnes physiques dans le cadre d'une activité personnelle ou domestique
- ✓ les **autorités publiques à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, d'exécution de sanctions pénales** ou de protection contre des menaces pour la sécurité publique et de prévention de telles menaces. Ces traitements font l'objet de la **Directive « Police justice »**

Un champ d'application territorial étendu

Le règlement s'applique dès lors qu'un de ces deux critères est présent :

- le responsable de traitement ou le sous-traitant est **établi sur le territoire de l'Union européenne**

OU

- le responsable de traitement ou le sous-traitant n'est pas établi sur le territoire de l'UE, **mais met en œuvre des traitement visant à fournir des biens et des services aux résidents européens ou à les surveiller (*monitor*)**

2 – Responsabilisation de nouveaux acteurs

Le sous-traitant

- obligations propres en matière de sécurité, de confidentialité et en matière d'*accountability*
- autorisation du RT pour recruter un ST
- tenue d'un registre
- obligation de conseil auprès du RT
- désignation d'un DPO

Le représentant légal

- point de contact de l'autorité
- tenue d'un registre
- mandat pour « être consulté en complément ou à la place du RT sur toutes les questions relatives aux traitements » (DPA, personnes, etc.)

Responsabilité conjointe

pour les sociétés qui « définissent de manière transparente leurs obligations respectives les de traitement conjoints »

3 – Renforcement du principe de licéité

- Le fondement juridique est rarement anticipé

- Particulièrement problématique en cas de réutilisation et de cessions de données

- au risque de détournement de finalité
- au principe de transparence et d'autodétermination
- à ne pas confondre pseudonymisation et anonymisation

Quel fondement juridique ?

Article 6 du règlement – licéité du traitement :

- **Consentement libre, spécifique et éclairé**
- **Exécution soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci (fréquent pour le commerce)**
- **Réalisation des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant**
- **Sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique**
- **Exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement**

Conditions de validité du le consentement

- action positive et claire : pas de consentement tacite ou passif ou de cases cochées par défaut ;
- la personne concernée doit être consciente du consentement donné et de sa portée : information claire et compréhensible ;
- consentement libre et distinct ;
- consentement spécifique ;
- consentement susceptible d'être retiré simplement.

Capacité à prouver le consentement

Le règlement impose de prouver **que la personne concernée a donné son consentement** :

- garantir aux utilisateurs une certaine **traçabilité**, => moyens de retracer l'historique des consentements et l'origine de la collecte des données ;
- permettre à la **CNIL de vérifier, dans le cadre de contrôles**, si le consentement des personnes a été valablement recueilli et correspond à l'utilisation qui a été faite des données par le responsable de traitement ;
- **Théoriquement c'est déjà le cas** : obligation actuelle d'indiquer l'origine des données sur demande et d'assurer le droit d'opposition en cascade…

Quid de l'intérêt légitime

Equilibre

Intérêt légitime du RT

Intérêts + droits et libertés fondamentaux des personnes

Equilibre résultant d'une analyse de :

1. **La nature et la source de l'intérêt légitime :**
   - exercice d'un droit fondamental ? intérêt public ? reconnaissance sociale, culturelle ou légale/réglementaire ?

2. **L'incidence sur les personnes concernées :**
   - nature des données (sensibles, publiques) et du traitement (diffusion, croisement, etc.) ;
   - attentes raisonnables de la personne concernée ;
   - statut du RT et de la personne concernée + rapport de force.

3. **Les garanties supplémentaires destinées à prévenir toute incidence**
   - minimisation des données ;
   - mesures techniques et organisationnelles, PbD ;
   - donner le pouvoir aux personnes concernées :
     - ✓transparence accrue,
     - ✓un droit général et inconditionnel de refuser le traitement,
     - ✓la portabilité des données, etc.

4 - Renforcement global des droits (aperçu)

Le renforcement des droits existants

- obligation générale de faciliter l'exercice des droits (fourniture d'une information claire, intelligible et aisément accessible)
- information renforcée (ex. transferts hors de l'UE, source des données, durée de conservation)
- droit d'accès précisé (ex. : possibilité d'introduire une réclamation devant une « CNIL »)
- droit à l'effacement et à l'oubli numérique confirmé

Les nouveaux droits

- la portabilité des données
- la limitation du traitement
- conditions particulières pour le traitement des données des enfants

Focus sur certains (nouveaux) droits

- **Droit à l'autodétermination informationnelle** (Loi Lemaire)

« Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant »

- **Droit d'opposition :**
  - Pour tout traitement fondé sur l'intérêt légitime et en particulier le ciblage : prise en compte sauf démonstration de motifs légitimes et impérieux ;
  - À tout moment pour les traitements aux fins de prospection ;
  - À ne pas faire l'objet d'une décision automatisée produisant des effets juridiques ou l'affectant de manière significative sauf si nécessaire à l'exécution d'un contrat ou relève du consentement, ou légalement fondé.

- **Droit à l'effacement**

- **Droit à la limitation du traitement**

- **Droit à la portabilité** :
  - récupération et réutilisation des données personnelles,
  - fournies par la personnes,
  - si elles ont été traitées de manière automatisée sur le fondement du consentement ou de l'exécution d'un contrat,
  - transmission dans un format structuré, couramment utilisé et lisible par machine.

- **Principes généraux applicables aux droits :**
  - possibilité de demander des informations supplémentaires pour confirmer l'identité de la personne exerçant les droits ;
  - notification aux destinataires et fourniture de listes sur demande ;
  - **réponse gratuite dans le mois**, + 2 mois si justifié et notifié à la personne.

5 – L'accountability à l'heure du Règlement

- Aujourd'hui => formalités préalables pour tout traitement => charge administrative et financière, peu efficace pour la protection des libertés ;
- Remplacées par des procédures et des mécanismes de responsabilisation

- ✓ **l'application des principes de privacy by design et privacy by default**
- ✓ **la conduite d'analyses d'impact, ou « DPIA » ;**
- ✓ **la tenue d'un registre des traitements mis en œuvre ;**
- ✓ **la notification de failles de sécurité ;**
- ✓ **la consultation de la CNIL - DPIA**
- ✓ **la certification de traitements**
- ✓ **et l'adhésion à des codes de conduites.**

Outils de conformité (d'accountability)

Registre des activités de traitement

Qui	Quand	Contenu	Autorité
RT ST De plus de 250 employés ****** < 250 employés si traitements à risques	Tous les traitements ********** Si mise en œuvre non occasionnelle de traitements à risques ou données sensibles	✓Nom du RT/Délégué à la protection ✓finalité du traitement, ✓catégorie de personnes, ✓transferts, ✓ mesures de sécurité ✓Etc.	Disponible sur demande

Outils de conformité

Notification des violations de données

Qui	A qui	Quand	Contenu
RT ST au RT	Autorité	✓sans délais, et au plus tard dans les 72 heures ✓à moins que la faille représente un risque peu probable concernant les droits et libertés des personnes.	✓La nature de la faille ✓Le nombre approximatif de personne concernée ✓Les mesures prises pour remédier à la faille
RT	Personne concernée	✓La faille représente un risque élevé pour la personne concernée ✓Le RT n'a pas pris des mesures garantissant que le risque élevé n'est plus susceptible de se matérialiser (ex : recours à des données codées) ✓La notification ne représente pas un effort disproportionné pour le RT notamment au regard du nombre de personnes concernées	Même contenu

La problématique

Des notifications variées

- Différents textes : RGPD, ePrivacy, eIDAS, NIS, Paquet Télécom, LPM…
- Différentes autorités de contrôle : ANSSI, CNIL, ARS…
- Différents processus pour gérer les incidents et les éventuelles notifications

→ Comment y voir plus clair ?

→ Comment factoriser ?

Outils de conformité

Conduite d'analyses d'impacts (PIA)

Qui	Quand	Contenu	Autorité
Le RT ✓Demande conseil au délégué à la protection ✓Demande l'avis des personnes concernées ou de leurs représentants au sujet du traitement prévu	✓Le traitement représente un **risque élevé pour les droits et libertés des personnes** ✓Le traitement concerne des données sensibles, données biométriques ✓Le traitement consiste en une évaluation systématique de la personne (profiling) ✓Le traitement consiste en une surveillance publique large échelle (vidéosurveillance)	✓Description systématique du traitement envisagé, sa finalité ✓Evaluation de la nécessité et de la proportionnalité ✓Evaluation du risque sur les droits et libertés des personnes concernées ✓Les mesures envisagées pour remédier aux risques (ex: mesures de sécurité)	✓Etablit, rend publique la liste des traitements devant faire l'objet d'une analyse d'impacts ✓Etablit, rend publique la liste des traitements ne devant pas faire l'objet d'une analyse d'impacts ✓Communication de la liste à l'EDPB ✓Consulté par le RT lorsque le traitement représente un risque élevé ✓Peut utiliser l'ensemble de ses pouvoirs

6 – L'approche par les risques / le PIA

- **Objectifs** :

  - ✓ garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;

  - ✓ Limiter les impacts pour les droits et libertés des personnes :

    - rejet automatique d'une demande de crédit en ligne ;
    - pratiques de recrutement en ligne sans aucune intervention humaine ;
    - dommages physiques, matériels ou un préjudice moral, en particulier ;
    - une discrimination, un vol, une perte financière, une atteinte à la réputation ;
    - tout autre dommage économique ou social important.

Compte tenu du contexte, de la nature etc.

- Nature :
  - ✓ données qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions philosophiques, l'appartenance syndicale ;
  - ✓ données génétiques ;
  - ✓ données concernant la santé ou la vie sexuelle ;
  - ✓ données relatives à des condamnations pénales, infractions, ou mesures de sûreté connexes ;
  - ✓ données relatives à des enfants, personnes vulnérables ;
  - ✓ volume important de données et / ou de personnes concernées.

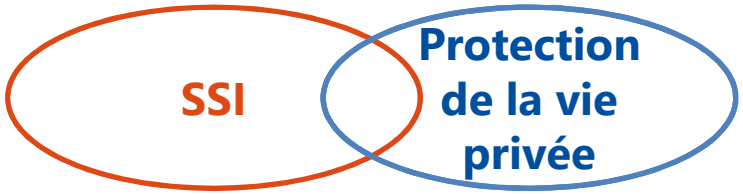
- Contexte et portée :
  - ✓ évaluation d'aspects personnels (analyse ou prédiction d'éléments concernant le rendement au travail, la situation économique, la santé, les préférences ou centres d'intérêt personnels, la fiabilité ou le comportement, la localisation ou les déplacements) ;
  - ✓ création ou utilisation de profils individuels ;
  - ✓ transfert international des données.

Et prendre des mesures adaptées

- Mesures correctives d'ordre « juridique » :
  - ✓ nécessité d'un fondement juridique fort notamment pour les données sensibles ;
  - ✓ information spécifique de la personne concernée ;
  - ✓ droit d'obtenir une intervention humaine, d'exprimer son point de vue, d'obtenir une explication quant à une décision automatisée et de la contester la décision (profilage) ;
  - ✓ minimisation des données, de la durée de conservation, de l'accessibilité.

- Mesures d'ordre organisationnel et technique :
  - ✓ notamment : les principes de protection des données dès la conception et de protection des données par défaut ;
  - ✓ réduire à un minimum le traitement des données à caractère personnel ;
  - ✓ pseudonymiser les données dès que possible ;
  - ✓ permettre à la personne concernée de contrôler le traitement des données ;
  - ✓ permettre au responsable du traitement de mettre en place des dispositifs de sécurité ou de les améliorer ;
  - ✓ intégrer les fabricants de produits, les prestataires de services, etc. ;
  - ✓ prise en considération dans le cadre des marchés publics.

Pourquoi étudier les risques vie privée de manière spécifique ?



Sécurité des systèmes d'information	Protection de la vie privée
Objectif : protéger l'organisme	Objectif : protéger les personnes concernées et leurs droits
Sujet de l'étude : ▪ Les informations manipulées au sein de l'organisme (dont les données à caractère personnel) ▪ Les processus métiers	Sujet de l'étude : ▪ Les données à caractère personnel confiées à l'organisme ▪ Les processus légaux
Impacts étudiés : image, juridiques (dont le non respect de la Loi Informatique & libertés), financiers…	Impacts étudiés : vie privée, identité humaine, libertés publiques…

7 – Le délégué à la protection des données

- Devient un véritable pilote de la conformité interne
- Le délégué à la protection des données est « *une personne possédant des connaissances spécialisées de la législation et des pratiques en matière de protection des données [qui] devrait aider le responsable du traitement ou le sous-traitant à vérifier le respect, au niveau interne, du présent règlement* » (cons. 97 du RGPD).
- Désignation obligatoire dans certains cas
- Compétences renforcées
- Exigence nouvelle de qualification
- Statut et responsabilités similaires à celles du CIL

Les cas de désignation obligatoire

- La désignation d'un délégué à la protection des données est obligatoire :
  - Si le traitement est effectué par une **autorité publique ou un organisme publics**

    => *Pour tout le secteur public (collectivités locales, Etat, établissements publics, etc.) quelque soit la nature du traitement*
  - Si les activités de base de l'organisme consistent en des traitements qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un **suivi régulier et systématique à grande échelle des personnes concernées** (*ex : profilage, secteur banque assurance, ciblage publicitaire, lutte contre la fraude et le blanchiment*)
  - Si les activités de base de l'organisme consistent en des traitement à **grande échelle** de **données sensibles** (article 9 du RGPD) ou de **données relatives aux condamnations et infractions spéciales** (article 10 du RGPD)

Les missions du délégué

- **Informe** et **conseille** l'organisme (ainsi que les salariés/agents) sur les obligations qui lui incombent en vertu du RGPD et d'autres dispositions de l'Union ou de l'Etat membre concerné = **mission actuelle du CIL**

- **Contrôle le respect du RGPD**, d'autres dispositions de l'Union ou de l'Etat membre concerné et des règles internes du RT ou du ST (sensibilisation, formation du personnel, audits,…) = **mission actuelle du CIL**

- Dispense des **conseils** en ce qui concerne **l'analyse d'impact (PIA ou EIVP)** relative à la protection des donnée et **vérifie son exécution** = **nouvelle mission**

- **Coopère** avec l'autorité de contrôle et fait office de **point de contact** pour les personnes concernées sur toute question en lien avec les traitements (les coordonnées du délégué devront figurer dans la mention d'information, voir les articles 13 et 14 du RGPD) = **mission actuelle du CIL**

- En tant que pilote de la conformité, il s'assure de la bonne tenue de **la documentation** relative aux traitements = **mission actuelle du CIL**

Les moyens du délégué

- **Des moyens à obtenir :**
  - Associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données
  - Doit disposer des ressources nécessaires à l'exécution de ses missions (notamment accès aux données et aux traitements) et au maintien de ses connaissances
  - Indépendance dans l'accomplissement de ses missions
  - Pas de sanction du fait de l'accomplissement de ses missions
  - Fait directement rapport au niveau le plus élevé de l'organisme

- **Sanctions :** en cas de non-respect des dispositions relatives au délégué, possible sanction par l'autorité de contrôle (CNIL) => **amende jusqu'à 10.000.000 € ou 2% du chiffre d'affaires total mondial** (article 83.4 du RGPD)

8 - La compétence étendue des CNILs

La confirmation et le développement des missions existantes

- Le contrôle du respect de l'application du texte ;
- La sensibilisation du public notamment sur les activités destinées spécifiquement aux enfants (cf. développement de la mission éducation numérique) ;
- Le conseil au Parlement, Gouvernement et autres institutions au sujet des mesures législatives ou réglementaires relatives à la protection des droits et libertés des personnes à l'égard d'un traitement ;
- La réalisation d'enquêtes ;
- Le traitement des réclamations introduites par une personne et l'information sur ses suites ;
- La délivrance de labels.

L'exercice de nouvelles missions

- L'adoption de clauses contractuelles types
- L'établissement et la mise à jour de la liste des traitements devant faire l'objet d'une analyse d'impact par le RT et la communication de cette liste au Comité Européen de la Protection des Données(CEPD) ;
- L'accompagnement du RT sur l'analyse d'impact menée et les mesures prises ;
- L'approbation des Règles d'entreprise contraignantes (BCR) ;
- **La suppression de la mission d'instruction des formalités préalables** (déclaration relative au traitement, normes simplifiées…).

Les nouveaux pouvoirs

Pouvoirs d'enquête :

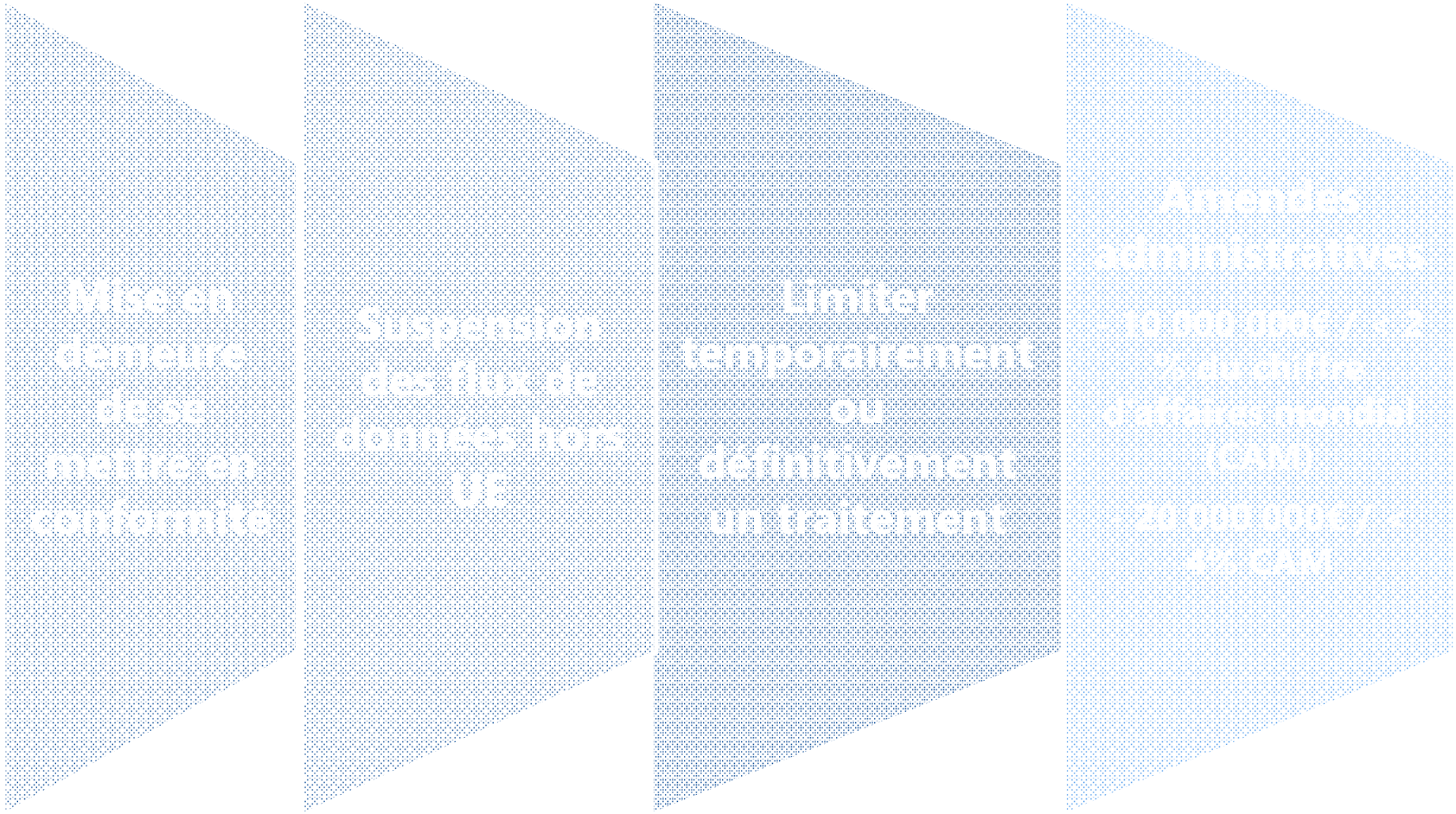
- Injonction de communication des informations nécessaires à l'accomplissement de ses missions ;
- *Mener des enquêtes sous la forme d'audits ;*
- Examen des certifications délivrées – possible retrait de la certification.

Mesures correctrices :

- Avertir, rappeler à l'ordre, ordonner une mise en conformité ;
- Ordonner la communication à la personne concernée d'une violation de données ;
- Imposer une limitation temporaire ou définitive voire une interdiction du traitement ou du transfert de données ;
- Ordonner respect des droits de rectification, opposition, limitation, etc.
- Retrait de certification ;
- Sanctions financières.

Des sanctions encadrées, graduées et renforcées

« Les sanctions sont effectives, proportionnées et dissuasives »



Des voies de recours déclinées

Droit à un recours juridictionnel contre un RT - ST

Droit à un recours juridictionnel contre une DPA

Droit à un recours collectif

Une personne peut mandater un tiers pour introduire une réclamation en son nom

Droit à réparation pour les usagers

Réparation en cas de dommage matériel ou immatériel

Montant des sanctions

< 10 000 000 EUR ou, dans le cas d'une entreprise, < 2 % du chiffre d'affaires annuel mondial

- ***consentement enfants***,
- *limitation des données pour traitement ne nécessitant pas d'identifier,*
- *application du PbDefault & Design,*
- *organisation de la responsabilité conjointe,*
- *représentant du RT non établi dans l'UE,*
- *encadrement de l'activité du sous-traitant, tenue du registre,*
- *coopération avec la CNIL, sécurité du traitement,*
- *notification de faille à la CNIL, communication de la faille à la personne,*
- *réalisation d'un DPIA, consultation de la CNIL sur DPIA,*
- *désignation d'un DPO qualifié et respect de ses missions,*
- *non respect de la procédure du certification;*

< 20 000 000 EUR ou, dans le cas d'une entreprise, < 4 % du chiffre d'affaires annuel mondial total

- *les principes de base d'un traitement (licéité, loyauté, proportionnalité, conditions applicables au consentement),*
- *respect des droits, encadrement des transferts respect disposition nationale spécifique, non respect injonction art. 58.*

Merci de votre attention !

Des questions ?