PROTECTION DES DONNÉES PERSONNELLES, PROCESSUS DE CONFORMITÉ RGPD ET DROIT EUROPÉEN
Guide rapide

TERRITOIRE OÙ S'APPLIQUE LE RGPD

Plus vaste que l 'Union Européenne.
ESPACE ÉCONOMIQUE EUROPÉEN, EEE (1992) =
→ 28 (27) PAYS DE UE
Allemagne, Autriche, Belgique, Bulgarie, Chypre, Croatie, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Lettonie, Lituanie, Luxembourg, Malte, Pays-Bas, Pologne, Portugal, République tchèque, Roumanie, Royaume-Uni (post-Brexit appliquera le RGPD ? à confirmer), Slovaquie, Slovénie, Suède

→ + 3 états de L'ASSOCIATION EUROPÉENNE DE LIBRE ÉCHANGE = AELE
• NORVÈGE
• LIECHTENSTEIN
• ISLANDE

La SUISSE a refusé de signer l'accord en 1992, c'est donc un pays tiers à l'Union Européenne (conséquences sur son statut au regard du RGPD)

LES PRINCIPES DU RGPD

• Licéité, loyauté, transparence
• Limitation des finalités
• Minimisation des données
• Exactitude
• Limitation de la conservation
• Intégrité et confidentialité des données
• Le traitement doit respecter les droits des personnes
• Transfert des données vers des pays tiers = hors EEE, art 44 à 49. Les justifier.

DÉFINITION D'UNE DONNÉE PERSONNELLE
ART 4-1 RGPD

Toute information sur

> personne physique (donc pas les données strictement de l'organisation, données de production…)
> identifiée
> ou identifiable =
• qui peut être identifiée
- directement

ou
- indirectement

par référence à
- un identifiant

exemples d'identifiants : (vaste…)
- un nom,
- un numéro d'identification,
- des données de localisation,
- un identifiant en ligne, ou
- un ou plusieurs éléments spécifiques propres à :
  - son identité physique,
  - physiologique,
  - génétique,
  - psychique,
  - économique,
  - culturelle ou
  - sociale

ATTENTION pas seulement les cookies !
ex : adresse IP, cookies, étiquettes d'identification par radiofréquence-RFI tags…

DÉFINITION D'UN TRAITEMENT DE DONNÉES PERSONNELLES

➔ Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés

➔ et appliquées à des données ou des ensembles de données personnelles, telles que :
• la collecte,
• l'enregistrement,
• l'organisation,
• la structuration,
• la conservation,
• l'adaptation ou la modification,
• l'extraction,
• la consultation,
• l'utilisation,
• la communication par transmission, la diffusion ou toute autre forme de mise à disposition,
• le rapprochement ou l'interconnexion,
• la limitation,
• l'effacement
• la destruction

RISQUES SUR LES DONNÉES SELON LE RGPD

• destruction
• perte
• altération
• divulgation non autorisée de données personnelles
> transmises,
> conservées ou
> traitées d'une autre manière
• ou de l'accès non autorisé à de telles données,
> de manière accidentelle ou
> illicite.

RISQUES POUR LES DROITS DES PERSONNES

Quels droits ?

➔ Droits fondamentaux dans l'Union Européenne (Charte des droits fondamentaux de l'Union Européenne)
Par ex :
> Droit à la vie privée
> Droit au respect du domicile,
> Droit au respect des communications
> Liberté d'expression et d'information
> Liberté d'entreprise
> Droit à la diversité culturelle, religieuse, linguistique
> Droit au recours effectif et à accéder à un tribunal

ART 32 RGPD : ASSURER LA SÉCURITÉ DES DONNÉES PAR DES MESURES TECHNIQUES ET ORGANISATIONNELLES

1) TENIR COMPTE DE L'ENVIRONNMENT GÉNÉRAL DU TRAITEMENT

• l'état des connaissances,
• des coûts de mise en œuvre
• de la nature,
• de la portée,
• du contexte
• des finalités du traitement
• des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques,

➔ le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées
➔ afin de garantir un niveau de sécurité adapté au risque

2) MESURES POSSIBLES SELON LES BESOINS , NON LIMITATIF

a) la pseudonymisation
le chiffrement

b) rechercher des moyens permettant de garantir

> la confidentialité
> l'intégrité
> la disponibilité
> la résilience constantes des systèmes et des services de traitement

c) rechercher des moyens permettant de rétablir

> la disponibilité des données personnelles
> et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique

d) prévoir une procédure visant à
> tester,
> analyser et
> évaluer

régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

3) À INCLURE DANS L'ÉVALUATION DU NIVEAU DE SÉCURITÉ APPROPRIÉ

ÉVALUER LES RISQUES POSSIBLES

• la destruction,
• la perte,
• l'altération,
• la divulgation non autorisée de données personnelles
> transmises,
> conservées ou
> traitées d'une autre manière

• ou l'accès non autorisé à de telles données
> de manière accidentelle ou
> illicite.

➔ UN CODE DE CONDUITE APPROUVÉ PAR L'AUTORITÉ CENTRALE (CNIL) ?
> (futurs) codes de conduite élaborés par les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants

OÙ TROUVER CES CODES DE CONDUITES EUROPÉENS ?

Le Comité européen de la protection des données (CEPD ou EDPB) consigne dans un registre tous les codes de les met à la disposition du public par tout moyen approprié.

→ UN MÉCANISME DE CERTIFICATION APPROUVÉ PAR UNE AUTORITÉ CENTRALE
ATTENTION : uniquement sur le processus de traitement par les responsables ou sous-traitants, pas sur les logiciels ou autres technologies

→ INCLURE UNE PROCÉDURE STRICTE DE CONTRÔLE DES ACCÈS AUX DONNÉES

Obligation pour le responsable ET le sous-traitant sur toutes les personnes qu'il contrôlent

LES 7 PRINCIPES DU PRIVACY BY DESIGN

1. Prendre des mesures proactives et non réactives, des mesures préventives et non correctives

→ prévoir et prévenir les incidents liés à l'atteinte de la vie privée avant même qu'ils ne se produisent

2. Assurer la protection implicite de la vie privée

→ Faire en sorte que les données personnelles soient protégées de manière automatique avec un paramétrage par défaut

3. Intégrer la protection de la vie privée dans la conception des systèmes et des pratiques

4. Assurer la protection de la vie privée sans nuire à la mise en œuvre d'autres fonctionnalités

5. Assurer la sécurité de bout en bout, pendant toute la période de conservation des renseignements

6. Assurer la visibilité et la transparence des éléments du système

7. Respecter la vie privée des utilisateurs

→ Application dans tous les aspects du traitement des données
→ Du recueil jusqu'à la destruction des données