Procédure et synthèse : RGPD et cybersécurité

1. Introduction au RGPD

Le Règlement Général sur la Protection des Données (RGPD) est une loi européenne entrée en application le 25 mai 2018. Son objectif est de renforcer la protection des données personnelles des citoyens européens et d'harmoniser les pratiques au sein de l'Union Européenne. Il s'applique à toute organisation publique ou privée traitant des données personnelles, qu'elle soit établie dans l'UE ou qu'elle cible des résidents européens.

2. Objectifs du RGPD

1. Renforcer les droits des personnes

2. Responsabiliser les acteurs traitant des données

3. Crédibiliser la régulation

3. Concepts clés

- Accountability : principe de responsabilité

- Privacy by design & by default : vie privée intégrée dès la conception

- Registre des traitements : documentation obligatoire des traitements de données

4. Données concernées

Données personnelles : nom, prénom, email, IP, géolocalisation, etc.

Données sensibles : santé, orientation sexuelle, opinions politiques, etc.

5. Bases légales d'un traitement

- Consentement explicite

- Exécution d'un contrat

- Obligation légale

- Sauvegarde des intérêts vitaux

- Mission d'intérêt public

- Intérêt légitime

6. Droits des personnes

1. Droit d'accès

2. Droit de rectification

3. Droit à l'effacement (oubli)

4. Droit à la portabilité

5. Droit à la limitation

6. Droit d’opposition

7. Procédure en cas de fuite de données

1. Mise en place d’une cellule de crise

2. Contenir et résoudre la faille

3. Notifier la CNIL sous 72h

4. Informer les personnes concernées si nécessaire

Loyauté et transparence

Vous devez informer les personnes concernées que vous traitez leurs données et comment vous le faites (art. 13 en cas de collecte directe et art. 14 en cas de collecte indirecte). Vous devez leur donner les informations suivantes :

Information	Exemples illustratifs
Vos coordonnées – le cas échéant les coordonnées de votre délégué à la protection des données	Votre adresse email et ou postale, un numéro de téléphone,…
La finalité du traitement (i.e. pourquoi vous traitez leurs données)	Gestion des salaires, prospection,….
La base juridique de votre traitement (cf. comme évoqué toute à l’heure). SI la base est votre intérêt légitime – vous devez indiquer quels sont ces intérêts	Cf. voir page précédente
Les destinataires / catégories de destinataires s’ils existent	CNS, Contributions directes, agence marketing, fiduciaire,…
Votre éventuelle **intention de transférer leurs données à un pays tiers**	Système IT opéré aux Etats-Unis

8. Acteurs clés

- RT : Responsable de traitement

- DPO : Délégué à la protection des données

- RSSI : Responsable de la sécurité des systèmes d'information

Les principales missions du DPO

- **Informer et de conseiller** le responsable de traitement de l'organisation et/ou le sous-traitant,
- **Diffuser une culture Informatique & Libertés** au sein de l'organisation ;
- **Contrôler le respect** du règlement et du droit national en matière de protection des données,
- **Conseiller l'organisation** sur la réalisation d'une analyse d'impact relative à la prot. des données
- **Coopérer** avec la CNIL et d'être le point de contact de celle-ci.
- S'assurer de la **bonne tenue** de la documentation relative aux traitements
- **Répondre aux demandes des utilisateurs** faisant valoir leurs droits (oubli, portabilité,…)

9. Traitements à risque

Exemples : surveillance, données de santé, données sensibles, transferts hors UE, etc.

10. Exemple de registre de traitement

Nom du traitement	Finalité	Base légale	Sensibilité
Gestion des salariés	Paiement des salaires	Intérêt contractuel	Oui
Transmission aux impôts	Paiement impôts	Intérêt légal	Non
Commandes fournisseurs	Réapprovisionnement	Intérêt contractuel	Non
Newsletter	Comprendre le client	Consentement	Non
Traitement client	Suivi commercial	Intérêt légitime	Oui

11. Documentation obligatoire

- Registre des traitements

- Mentions légales et politiques de confidentialité

- Courriers de notification

- Études d'impact et transferts hors UE

RGPD : se préparer en 6 étapes