MEDEF

4. RESPONSABILITE (*Accountability*)

1. Qu'est-ce que l'*accountability* ?

Le principe d'*accountability* implique **la responsabilisation des acteurs économiques, en renforçant leurs obligations tout en les incitant à jouer un rôle actif dans le contrôle de la conformité de leurs traitements**. L'une des conséquences les plus significatives est la suppression des déclarations préalables à la CNIL.
Les entreprises doivent toutefois **s'assurer et être en mesure de démontrer** que le traitement est effectué conformément au RGPD. Elles doivent donc mettre en place une politique et des processus internes pour vérifier la conformité des traitements.

2. Qui sont les acteurs concernés ?

(Co)Responsable du traitement

Le responsable de traitement (ou « *controller* ») est défini par la loi, ce qui signifie qu'un contrat ne peut pas prévoir que le responsable sera un tiers. En revanche, **plusieurs personnes peuvent être désignées responsables conjoints d'un traitement et elles** doivent définir leur périmètre de responsabilité respective. Les personnes concernées peuvent toutefois exercer leurs droits indifféremment auprès de chaque responsable conjoint.

Sous-traitant

Les sous-traitants (ou « *processors* »), même s'ils ne sont pas directement soumis au principe d'*accountability*, sont également **soumis à certaines obligations afin d'aider le responsable de traitement à contrôler la sécurité et la conformité de ses traitements**. Ils ont par ailleurs des obligations qui leur sont propres lorsqu'ils sont amenés à traiter régulièrement et à grande échelle des données personnelles (tenue d'un registre de traitements, désignation d'un DPO notamment).

Exemples de coresponsabilité

…lorsqu'une plateforme de partage de données est développée en partenariat par deux entreprises

Fournisseur d'électricité

Objet connecté

…lorsqu'une application permet le suivi en temps réel de sa consommation d'électricité

Exemples de sous-traitance

…lorsqu'une entreprise utilise un service de cloud ou confie le développement de solutions informatiques à un tiers.

…lorsqu'une entreprise utilise un service de coffre-fort numérique ou confie la gestion de la paie à un tiers.

3. Quelles sont les obligations des différents acteurs ?

➢ Responsable de traitement (« *Controller* »)

Je collecte ou utilise des données personnelles au sein de mon entreprise. **Que dois-je mettre en place et quelles sont mes obligations en tant que responsable de traitement** ?

1. Mettre en place des mesures internes pour s'assurer et démontrer la conformité des traitements :

- Mettre en place une politique interne de protection des données personnelles
- Désigner des personnes dédiées à la protection des données personnelles (DPO, juristes, informaticiens…)
- Elaborer des règles ou processus internes (reporting, gestion des traitements, comité de validation…)
- Adopter des codes de conduite, participer à des mécanismes de certification (labels CNIL…)
- Mettre en place une politique interne de sécurité de l'information (contrôles d'accès, classification des informations, sauvegardes, antivirus et anti-malware, tests de vulnérabilité…) – PSSI
- Sensibiliser et former l'ensemble des collaborateurs (conseillers clients, RH, DSI…)
- Fournir les informations nécessaires aux personnes concernées (*cf. fiche 2*)
- Respecter et veiller au respect des droits des personnes concernées (*cf. fiche 3*)
- Intégrer la protection des données personnelles dès la conception des projets, programmes ou SI (« ***Privacy by design*** »)

2. Vérifier le respect des grands principes en matière de traitement de données personnelles :

- **Licéité** : le traitement doit reposer sur le consentement de la personne, un contrat, une obligation légale, une mission d'intérêt public ou encore l'intérêt légitime du responsable (*cf. fiche 1*)
- **Transparence et loyauté** : les personnes concernées doivent être informées de l'existence et des modalités du traitement.
- **Limitation des durées de conservation** : les données doivent être conservées pour la durée strictement nécessaire.
- **Limitation des finalités** : les données personnelles doivent être collectées pour des finalités déterminées, explicites et légitimes et ne pas être réutilisées d'une manière incompatible avec ces finalités initiales.
- **Minimisation des données** : les données personnelles collectées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités.
- **Exactitude** : les données personnelles doivent être exactes et raisonnablement tenues à jour.

3. Vérifier les relations avec les sous-traitants :

- Vérifier l'existence d'un contrat de sous-traitance définissant les modalités de traitement des données personnelles (objet, durée, finalité du traitement) et les obligations du sous-traitant (notamment sécurité et lieu d'exécution du contrat)
- Vérifier que les sous-traitants présentent des garanties suffisantes pour le traitement de données personnelles (notamment en matière de sécurité et du lieu d'hébergement)

4. Désigner un délégué à la protection des données (*Data Protection Officer* - DPO) interne ou extérieur à l'organisme

- Le DPO est obligatoire lorsque les activités de base consistent en un suivi régulier et systématique à grande échelle de données ou en un traitement à grande échelle de données particulières (données biométriques, de santé, révélant l'origine raciale ou ethnique, les opinions politiques, syndicales, religieuses ou philosophiques, l'orientation sexuelle…)
- Un groupe d'entreprises peut désigner un DPO unique

5. Tenir un registre des activités de traitement sous forme écrite ou électronique :

- Cette obligation concerne les entreprises ou organisations de plus de 250 salariés, sauf si les traitements effectués par les petites structures sont réguliers et présentent un risque pour les personnes concernées (par exemple : profilage, publicité ciblée), ou s'ils portent sur des données particulières (telles que les données biométriques, données de santé ou encore les données portant sur les origines raciales ou ethniques, les opinions politiques, syndicales ou religieuses, etc)
- Le registre doit mentionner pour chaque traitement le nom et les coordonnées du responsable de traitement (et le cas échéant du DPO désigné), les finalités du traitement, les catégories de personnes concernées (salariés, clients…), les destinataires des données, les éventuels transferts de données personnelles, les délais de conservation et les mesures de sécurité mises en place

6. Mettre en place les mesures appropriées pour assurer la sécurité des traitements (*cf. fiche 5*)

- Assurer la confidentialité des données personnelles (pseudonymisation, chiffrement des données ou tout autre moyen)
- Assurer l'intégrité des données (contre la destruction, la perte, l'altération des données)
- Assurer la disponibilité des données et mettre en place des moyens permettant un rétablissement dans des délais appropriés
- Effectuer des tests, analyses et évaluations réguliers de l'efficacité des mesures mises en place
- Utiliser par exemple des codes de conduite approuvés par la CNIL (référentiels, pack de conformité…)
- Vérifier la mise en place de mesures de sécurité appropriées par les sous-traitants (audit)

7. Notifier les incidents de sécurité concernant des données personnelles (*cf. fiche 6*)

- Mettre en place une procédure de notification des violations de données personnelles à la CNIL
- Notifier ces incidents à la CNIL, si possible dans les 72h, lorsqu'il existe un risque pour les personnes
- Alerter les personnes concernées de ces incidents lorsqu'il y a un risque élevé pour leurs droits

8. Faire des analyses d'impact pour les traitements les plus sensibles et, lorsque cette analyse révèle un risque élevé pour les personnes concernées, consulter la CNIL *(cf. fiche 7)*

➢ Sous-traitant (« *Processor* »)

Je traite des données personnelles pour le compte d'une entreprise. **Que dois-je mettre en place et quelles sont mes obligations en tant que sous-traitant** ?

1. Vérifier les relations avec ses propres sous-traitants :
- Ne pas sous-traiter sans l'autorisation écrite préalable du responsable de traitement
- Vérifier que les sous-traitants présentent des garanties suffisantes pour le traitement de données personnelles
- Vérifier l'existence d'un contrat de sous-traitance définissant les modalités de traitement des données personnelles (objet, durée, finalité du traitement) et les obligations du sous-traitant (sécurité, lieu de réalisation du traitement…)

2. Agir conformément aux instructions du responsables de traitement (en fonction du contrat de sous-traitance) **:**
- Ne traiter les données que sur instruction du responsable de traitement (y compris pour les transferts de données vers des pays hors Union européenne)
- Veiller au respect de la confidentialité des données par son personnel
- Aider le responsable de traitement à s'acquitter de ses obligations en matière de protection des données personnelles
- Supprimer ou rendre au responsable de traitement les données personnelles au terme de la prestation de services et détruire les copies existantes de ces données
- Mettre à la disposition du responsable de traitement toutes les informations nécessaires pour démontrer le respect des obligations et pour la réalisation d'audits ou de contrôles

3. Tenir un registre des activités de traitement effectuées pour le compte d'un responsable de traitement (sous forme écrite ou électronique) :
- Cette obligation concerne les entreprises ou organisations de plus de 250 salariés, sauf si les traitements effectués par les petites structures sont réguliers et présentent un risque pour les personnes concernées (par exemple : profilage, publicité ciblée), ou s'ils portent sur des données particulières (telles que les données biométriques, données de santé ou encore les données portant sur les origines raciales ou ethniques, les opinions politiques, syndicales ou religieuses, etc)
- Le registre doit mentionner pour chaque traitement le nom et les coordonnées des sous-traitants et du responsable de traitement (et le cas échéant du DPO désigné), les éventuels transferts de données personnelles et les mesures de sécurité mises en place

4. Mettre en place les mesures appropriées pour assurer la sécurité des traitements (*cf. fiche 5*)
- Assurer la confidentialité des données personnelles (pseudonymisation, chiffrement des données ou tout autre moyen)
- Assurer l'intégrité des données (contre la destruction, la perte, l'altération des données)
- Assurer la disponibilité des données et mettre en place des moyens permettant un rétablissement dans des délais appropriés
- Effectuer des tests, analyses et évaluations réguliers de l'efficacité des mesures mises en place
- Utiliser par exemple des codes de conduite approuvés par la CNIL (référentiels, packs de conformité…)
- Vérifier la mise en place de mesures de sécurité appropriées par ses propres sous-traitants

5. Notifier les incidents de sécurité concernant des données personnelles au responsable de traitement (*cf. fiche 6*)
- Notifier toute violation de données personnelles au responsable de traitement dans les meilleurs délais
- Mettre à disposition du responsable de traitement les informations nécessaires pour le reporting auprès de la CNIL

6. Désigner un délégué à la protection des données (*Data Protection Officer* - DPO) interne ou extérieur à l'organisme
- Le DPO est obligatoire lorsque les activités de base consistent en un suivi régulier et systématique à grande échelle de données ou en un traitement à grande échelle de données particulières (données biométriques, de santé, relatives à l'origine raciale…)

4. Quels sont les risques et sanctions ?

Pour le responsable de traitement	Pour le sous-traitant (pour ses obligations propres)
Action judiciaire (devant les tribunaux) : - Obligation de **cesser une violation de données personnelles (par décision de justice)** - **Sanctions pénales** : jusqu'à 5 ans d'emprisonnement et 300.000 € d'amende pour les personnes physiques et 1.500.000 € d'amende pour les personnes morales	**Action judiciaire** (devant les tribunaux) : - Obligation de **cesser une violation de données personnelles (par décision de justice)** - **Sanctions pénales** : jusqu'à 5 ans d'emprisonnement et 300.000 € d'amende pour les personnes physiques et 1.500.000 € d'amende pour les personnes morales
Amendes administratives (prononcées par la CNIL) : - Jusqu'à 10.000.000 € ou 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent pour une entreprise - Jusqu'à 20.000.000 € ou 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent pour une entreprise pour les manquements les plus graves	**Amendes administratives** (prononcées par la CNIL) : - Jusqu'à 10.000.000 € ou 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent pour une entreprise - Jusqu'à 20.000.000 € ou 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent pour une entreprise pour les manquements les plus graves