RGPD AVOIR TOUJOURS LES BONS RÉFLEXES

Fiche n°6

Quels sont les documents nécessaires à la mise en conformité RGPD ?

CONTEXTE

La conformité au RGPD impose un certain nombre de **règles qui se traduisent par les documents directement tirés du RGPD** (ex. le registre de traitement) et d'autres qui sont déduits d'autres obligations.

En cas d'audit, la non présentation des documents exigés **peut conduire à une amende.**
Toutefois, **la démonstration d'une démarche** de progression dans la réalisation des documents concernés peut **réduire ce risque.**

L'ESSENTIEL À RETENIR

Pour prouver votre conformité, constituez et regroupez la documentation nécessaire.

Réexaminez et actualisez régulièrement les actions et documents réalisés à chaque étape pour assurer une protection des données en continu.

ACTIONS À RÉALISER

Constituer un registre de traitements de données

Réaliser les Analyses d'Impact relatives à la Protection des Données pour les traitements susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes

Informer les personnes (via la DRH pour les salariés)

Prévoir les documents de sensibilisation / formation

Définir une procédure pour la réponse à la demande d'accès

Avoir les clauses contractuelles requises en cas de transfert hors UE (voir Fiche Réflexe n°2)

Préparer les clauses à insérer dans les contrats de sous / co-traitance

Réaliser une cartographie des actions et des processus (penser à celles de l'ISO 9001)

POUR ALLER PLUS LOIN

Par où commencer :
https://www.cnil.fr/fr/rgpd-par-ou-commencer

Modèle de registre simplifié proposé par la CNIL :
https://www.cnil.fr/fr/la-cnil-publie-un-nouveau-modele-de-registre-simplifie

Documenter la conformité :
https://www.cnil.fr/fr/documenter-la-conformite

Les points de vigilance :
https://www.cnil.fr/fr/rgpd-points-de-vigilance

Conformité RGPD : comment recueillir le consentement des personnes ? :
https://www.cnil.fr/fr/conformite-rgpd-comment-recueillir-le-consentement-des-personnes

Comment déterminer si une AIPD est nécessaire ? :
https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-aipd

POINTS DE VIGILANCE

Le respect du droit des personnes

(Les informer et leur permettre d'exercer facilement leurs droits).

Le traitement des données dites sensibles

(Origine prétendument raciale ou ethnique, opinions politiques, philosophiques ou religieuses, relatives à l'appartenance syndicale, concernant la santé ou l'orientation sexuelle, génétiques ou biométriques).

Un traitement qui aurait pour objet ou pour effet l'évaluation d'aspects personnels ou notation d'une personne

- Scoring financier ;
- Une prise de décision automatisée ;
- La surveillance systématique de personnes (exemple : télésurveillance) ;
- Le traitement de données sensibles (exemple : santé, biométrie, etc.) ;
- Le traitement de données concernant des personnes vulnérables (exemple : mineurs) ;
- Le traitement à grande échelle de données personnelles ;
- Le croisement d'ensembles de données ;
- Des usages innovants ou l'application de nouvelles technologies (exemple : objet connecté) ;
- L'exclusion du bénéfice d'un droit, d'un service ou contrat (exemple : liste noire).

Le signalement à la CNIL

Des violations de données personnelles dans les 72 heures si cette violation est susceptible de représenter un risque pour les droits et libertés des personnes concernées. Si ces risques sont élevés pour ces personnes, vous devrez les en informer.

RISQUES

Les risques marketing et commerciaux :

- Des usagers ou des consommateurs qui interrogent les entreprises sur ce qu'elles font de leurs données personnelles et qui faute de réponse risquent de saisir la CNIL.
- Des clients qui pourraient préférer signer des contrats avec des concurrents conformes.

Le risque d'image :

- Perte de confiance des clients, des prospects voire des collaborateurs.