Recommandations sur les règles de gestion pour la mise en conformité RGPD

Février 2024 – Manon DARGET

1) Désignez un DPD (Délégué à la Protection des Données)

Dans le cadre de la mission de mise en conformité RGPD de l'entreprise Dev'Immédiat, un délégué à la protection des données a été désigné temporairement. Afin que cette étape cruciale pour votre entreprise se déroule avec succès, il serait très intéressant de désigner, dès à présent, le futur DPD. Épaulé par le DPD temporaire, il pourra suivre l'entièreté du processus et la prise de poste se fera plus aisément de cette manière.

Intégrer les équipes dès la mise en place des éléments de mise en conformité est le meilleur moyen de responsabiliser vos équipes à la gouvernance des données.

2) Constituez un registre de vos traitements de données

Afin d'avoir une vision globale sur le traitement des diverses données au sein de votre entreprise, il est important de cartographier vos traitements de données.

Pour ce faire, il faut que vous identifiiez les activités principales de votre entreprise utilisant des données personnelles.

Lorsque vous avez listé vos différentes activités, vous devez indiquer, a minima, pour chacune d'entre elles :

- L'objectif de cette collecte de données
- Les catégories de personnes concernées (client, employé, etc.)
- Les catégories de données exploitées (nom, prénom, date d'obtention du permis, etc.)
- Les services/catégories de destinataires accédant à ces données
- Les transferts de données personnelles vers des pays tiers
- La durée de conservation
- Une description générale des mesures de sécurités mise en œuvre

Dans le cas où vous opérez des traitements de données en tant que sous-traitant, vous devez tenir un deuxième registre listant les traitements que vous effectuez pour le compte de vos clients.

Le registre des activités de traitement devra comporter le nom ainsi que les coordonnées de votre entreprise et le nom et prénom de votre délégué à la protection des données.

Pour plus d'informations :

https://www.cnil.fr/fr/RGPD-le-registre-des-activites-de-traitement

https://www.cnil.fr/fr/cartographier-vos-traitements-de-donnees-personnelles

3) Minimisez vos données

Maintenant que votre registre a été établi, vous allez pouvoir vous appuyer dessus pour trier vos données. Pour chaque activité de votre registre, posez-vous les questions suivantes :

- Les données traitées sont-elles nécessaires à votre activité ?
- Les données traitées sont-elles sensibles ? *Si oui, avez-vous le droit de les traiter ?*
- Les données sont-elles uniquement accessibles par les personnes en ayant besoin ?

- Les données sont-elles conservées au-delà de la durée définie et nécessaire ?

Il est important de minimiser la collecte de données en ne collectant que les données utiles.

Pour plus d'informations :

https://www.cnil.fr/fr/definition/donnee-sensible

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

4) Respectez les droits des personnes

Vous faites l'objet d'une obligation d'information et de transparence à l'égard des personnes dont vous traitez les données, il est donc **important** de les **informer** de la **collecte** de leurs **données** mais également de leur permettre **d'exercer leurs droits** facilement.

Qu'importe le support utilisé pour la collecte de données, celui-ci doit afficher distinctement une mention d'information. Cette mention d'informations doit permettre aux personnes de savoir :

- La finalité de la collecte, pourquoi les données sont-elles collectées ?
- Si vous transférez des données en dehors de l'Union Européenne (si oui, dans quels pays ?)
- Qu'est-ce qui vous autorise à collecter et traiter ces données ?
- Qui a accès à ces données ?
- La durée de conservation de ces données
- Les modalités leur permettant d'exercer leurs droits

Cette mention d'informations peut être regroupée dans une page « **Politique de confidentialité »**, vers laquelle vous ajouterez le lien à chaque point de collecte.

Les personnes dont vous collectez les données ont des droits dessus (droit d'accès, de rectification, d'opposition, etc.), il est important de mettre en place un processus leur garantissant l'exercice de leurs droits de manière aisée.

Pour plus d'informations :

https://www.cnil.fr/fr/rgpd-exemples-de-mentions-dinformation

https://www.cnil.fr/fr/les-droits-des-personnes-sur-leurs-donnees

5) Sécurisez vos données

Il est primordial de sécuriser vos données, autant pour protéger votre patrimoine de données que pour garantir la sécurité des personnes dont vous avez collecté les données.

Mettez en place des bonnes pratiques au sein de votre organisme aussi bien informatiques que physiques (choisir des mots de passes sécurisés, chiffrer les données si nécessaire, effectuer des sauvegardes, etc.)

Si vous subissez une violation de données, vous disposez de 72 heures pour la signaler auprès de la CNIL. Si les risques sont considérés comme élevés pour les personnes concernées par ces données, vous devez les informer de cette violation.

Pour plus d'informations :

https://cyber.gouv.fr/dix-regles-dor-preventives

https://cyber.gouv.fr/publications/la-cybersecurite-pour-les-tpepme-en-treize-questions