Livret Conformité Protection des données et Sécurité

AVRIL 2024

Avant-propos

La **protection des données personnelles**, vous en entendez beaucoup parler, surtout depuis l'entrée en application du règlement relatif à la protection des données personnelles (le "**RGPD**") le 25 mai 2018 mais au fond... vous ne savez pas vraiment ce que cela implique, concrètement, pour vous, dans vos missions.

Le RGPD s'applique aussi aux freelances. C'est une vraie opportunité de vous démarquer à condition de bien comprendre en quoi vous êtes concerné(e) et ce qu'on attend de vous.

Sommaire

Chapitre 1

La réglementation applicable

& Les grands principes en matière de protection des données

Le traitement des données personnelles est encadré par le **RGPD,** en vigueur depuis le 25 mai 2018, mis en oeuvre au sein de tous les pays de l'UE

Objectifs

Renforcer le droit des personnes
Responsabiliser les acteurs
Coopération renforcée entre les pays de l'UE

Qui est concerné?

Tout organisme :

- **qui est établi sur le territoire de l'UE**
- **dont l'activité cible des résidents européens**

[Lien](#) vers le texte

Qu'est-ce qu'une **donnée personnelle**

Une donnée personnelle est "toute information se rapportant à une personne physique identifiée ou identifiable"

Quelques exemples :

- Nom et prénom
- Cookies
- Adresse IP
- Photos et vidéos
- Coordonnées de prospects
- Revenu
- Données des préposés des clients
- Adresse email et postale

Qu’est-ce qu’un traitement de données personnelles

Un **traitement de donnée personnelles** est une opération ou ensemble d’opérations portant sur des données personnelles quelque soit le procédé utilisé.

- Collecte
- Consultation
- Enregistrement
- Utilisation
- Enregistrement
- Communication
- Modification
- Suppression

Principe de finalité

Les informations des personnes ne peuvent être utilisées que dans un but précis, légal et légitime.

Principe de proportionnalité

Les informations doivent être pertinentes et strictement nécessaires au regard de la finalité du traitement.

Durée de conservation limitée

Une durée de conservation précise doit être fixée, en fonction du type d'information et de la finalité du traitement.

Sécurité et confidentialité

Seules les personnes autorisées doivent pouvoir avoir accès aux informations sur des personnes, ces informations sont confidentielles et doivent être sécurisées.

Droits des personnes

Chaque personne dispose de droit quant à l'utilisation de leurs données, à savoir : droit d'accès, droit de rectification, à l'effacement, d'opposition, droit de retrait du consentement, droit de réclamation, droit à la portabilité.

Le droit des personnes sur leurs données - Source CNIL
Les six grands principes du RGPD - Source CNIL

Quels sont les rôles envisagés par le RGPD

Le Responsable de Traitement détermine la finalité et les moyens du traitement.

Le Sous-traitant traite les données pour le compte et sur instructions du Responsable de Traitement.

En tant que Freelance, vous êtes Sous-traitant du Client, agissant sous ses instructions en ce qui concerne les données traitées dans le cadre de votre mission.

Les obligations du Sous-traitant :

- Assure la protection et la confidentialité des données personnelles du Responsable de Traitement qu'il traite pour son compte
- La sous-traitance ultérieure est interdite sans accord express du Responsable de Traitement
- Ne peut réutiliser les données pour une autre finalité que celle déterminée par le Responsable de Traitement
- Doit assister le Responsable de Traitement

Vous devez respecter ces obligations en manipulant les données personnelles du client, en tant que Sous-traitant au sens du RGPD.

Travailler avec un sous-traitant - Source CNIL

Chapitre 2

Assurer sa conformité

Les mesures à mettre en oeuvre pour assurer votre conformité et protéger votre système d’information

Les étapes de la conformité

Constituez un **registre des traitements** de données réalisés en identifiant les principales opérations menés dans le cadre de la mission : objectif, catégories de données utilisées, qui a accès aux données, la durée de conservation.

Faites le tri : ne traitez que des données nécessaires à la réalisation de votre mission et limitez en l'accès.
Posez-vous la question "ai-je le droit de traiter cette donnée ?" notamment s'il s'agit de données sensibles.

Respectez le droit des personnes : ayez connaissance des droits des personnes et gardez les en tête à chaque fois que vous manipulez des données personnelles.

Sécurisez les données : mettez à jour vos antivirus, utilisez des mots de passe forts et complexes, effectuez des sauvegardes, mettez en place des mesures de chiffrement lorsque cela est possible.

Exemples de mesures d'hygiènes informatiques

Installer un pare-feu ("firewall") et un antivirus

Mettre à jour régulièrement ses logiciels et outils

Prévoir un mécanisme de verrouillage automatique de session en cas de non-utilisation de l'ordinateur pendant un temps donné

Réaliser des sauvegardes régulières

Limiter la connexion de supports mobiles (clé USB, disques durs externes)

Désactiver "l'autorun" depuis les supports mobiles

Assurer votre conformité en 4 étapes - Source CNIL

Chapitre 3

Réalisation une mission via Malt

Vos obligations en matière de protection et de sécurité des données personnelles

En tant que Freelance

Vous réalisez la mission pour le compte et sous instructions (au sens du RGPD) du client, le Responsable de Traitement ;

Vous pouvez être amené à effectuer des traitements de données personnelles dans le cadre de l'exécution de la mission ;

Vous devez veiller à assurer la protection et la sécurité des données personnelles.

Les instructions classiquement données par le client

Ne traitez que les données selon la finalité définie par le client.

Tenir un registre et être prêt à être audité.

Ne conserver les données uniquement pour le temps de réalisation de la prestation, et les supprimer ou les retourner une fois la mission réalisée.

Prendre toutes les précautions utiles pour assurer la sécurité des données.

Assister le client en cas d'exercice d'un droit par une personne concernée ou en cas de contrôle des autorités.

Informer le client en cas de violation des données

Vous devez informer le client si les données qui vous ont été confiées sont, de manière accidentelle ou illicite, détruites, perdues, altérées, divulguées ou accédées par des personnes non autorisées.

Vous n'avez que peu de temps : entre 48h et 72h en moyenne.
**Nous vous invitons à vérifier au sein de votre contrat les conditions de cette notification.*

La notification doit contenir les informations suivantes:

- La nature de la violation ;
- Les catégories et le nombre approximatif de personnes concernées ;
- Un point de contact auprès duquel des informations complémentaires peuvent être obtenues ;
- Les conséquences probables de la violation ;
- Les mesures prises pour y remédier ou atténuer ses conséquences.

Les violations de données personnes - Source CNIL

Le sort des données une fois la mission terminée

Les réflexes à avoir :

- Suppression des données auxquelles le client vous a donné accès pour la réalisation de votre mission et toutes copies éventuelles (sauf obligation légale)

- Ne pas télécharger de document interne du client sur un support externe (ex: envoi vers votre adresse email personnelle)

- Remise d'un certificat de destruction si le client en fait la demande

- Restitution du matériel du client prêté durant le temps de la mission

- Anonymiser les données qui ne sont pas soumis à la propriété intellectuelle

Chapitre 4

Travail à distance : les bonnes pratiques

Ce que vous devez lire et implémenter avant de commencer

Les risques inhérents au travail à distance

Points de vigilance :
Quand vous travaillez en dehors des locaux du client, nous ne disposez pas des moyens de protection habituellement mis en oeuvre au sein des locaux de l'entité (*à votre domicile, dans les transports, dans un espace de co-working*).

Dans tous ces lieux de travail non maîtrisés par le client, les risques sont exacerbés :

- Perte ou vol de matériel
- Accès illégitime au système d'information
- Compromission du matériel et des informations s'y trouvant
- Perte de confidentialité ou d'intégrité

Les questions à se poser avant :

La mission : Les conditions de réalisation de la mission me permettent-elles de travailler à distance ?

Autorisation : Le travail à distance peut ne pas être autorisé en raison du niveau de sensibilité des données traitées, de contraintes réglementaires ou parce qu'il existe des restrictions liées au métier (utilisation d'un matériel spécifique).

Paramétrages : Est-ce que le client impose la configuration de certains paramètres afin de travailler à distance ? *prenez- en connaissance.*

Les bons réflexes à avoir

Confidentialité : disposez un filtre écran de confidentialité sur votre poste de travail lors de vos déplacements ;

Absence : ne vous séparez pas de votre matériel ;

Mot de passe : utilisez des mots de passes forts et complexes et différents pour chacun de vos comptes ou utilisez un gestionnaire de mot de passe ;

Verrouillage : réduisez la durée d'inactivité avant verrouillage automatique de votre matériel ;

WIFI : ne vous connectez pas à des WIFIS publics, privilégiez le partage de connexion et utilisez un VPN ;

Périphérique : ne connectez pas à votre matériel des périphériques informatiques qui vous sont inconnus.

BYOD : quelles sont les bonnes pratiques - Source CNIL

BONUS

Les ressources à votre disposition

Les ressources mis à disposition par Malt

Nous vous invitons à lire attentivement ce **Livret Conformité** et la **Check-list Sécurité** mis à votre disposition qui reprend l'ensemble des exigences de sécurité auxquelles vous devez vous conformez dans le cadre de votre mission.

Les ressources externes

Formation

De nombreux MOOC existent que nous vous encourageons à suivre pour vous former aux bases de la protection des données, dont celui de la CNIL (https://www.cnil.fr/fr/comprendre-le-rgpd/le-mooc-de-la-cnil-est-de-retour-dans-une-nouvelle-version-enrichie)

MOOC de l'ANSSI : https://secnumacademie.gouv.fr/

Lien utiles

Comprendre le RGPD :
https://www.cnil.fr/fr/comprendre-le-rgpd

Sécuriser son poste de travail :
https://www.cnil.fr/fr/securite-securiser-les-postes-de-travail

Checklist TPE/PME :
https://www.cnil.fr/sites/cnil/files/atoms/files/check-list_rgpd_pour_les_tpe-pme.pdf