ENGAGEMENT N°17

RELATIONS CLIENTS

Protéger les données et la vie privée des personnes.

Traitement des données clients.

Le personnel est formé et sensibilisé à l'usage légal des données personnelles . La déclaration CNIL pour la vidéosurveillance est faite et est à jour.	Le point audité est conforme à la loi GDPR (General Data Protection Regulation) de l'UE applicable à compter du 25 mai 2018.	Une zone de confidentialité est prévue dans les lieux d'échanges de données personnelles.	Mise en place d'un suivi régulier.

J'APPRENDS

Explication et contexte

Pour comprendre comment répondre à cet engagement, il est nécessaire dans un premier temps de revenir sur les termes de gestion des données et de protection des données personnelles. **Comment les entreprises et les administrations doivent et peuvent répondre à cette obligation ?**

Une donnée personnelle a été définie selon la CNIL comme "toute information se rapportant à une personne physique identifiée ou identifiable […] En effet, il est possible d'identifier une personne par son nom et/ou par son prénom, par une photo, mais aussi par son numéro de téléphone, sa plaque d'immatriculation, son numéro de sécurité sociale, son adresse postale, son adresse e-mail."

Lorsqu'une entreprise collecte des données personnelles elle doit le faire avec un objectif précis, dans une durée limitée.

Point réglementaire

La France a légiféré le 6 janvier 1978 avec la loi n°78-17 "Informatique et Libertés". Puis le 25 mai 2018 le Règlement Général de la Protection des Données (RGPD) a vu le jour pour harmoniser les pratiques au niveau de l'Union Européenne.

Ainsi c'est avec la loi n°2018-493 du 20 juin 2018 qui a permis la mise en œuvre concrète du RGPD et de la Directive "police-justice" applicable aux fichiers de la sphère pénale afin de mettre en conformité le droit national avec le cadre juridique européen.

Pour être conforme au RGPD il faut informer les personnes et assurer la transparence. Le RGPD impose une information concise, transparente, compréhensible et aisément accessible des personnes concernées. Ces informations sont définies aux articles 12, 13 et 14 du RGPD.

Les "modalités de fourniture et de présentation de cette information doivent être adaptées au contexte". "La transparence permet aux personnes concernées de connaître la raison de la collecte des différentes données les concernant ; de comprendre le traitement qui sera fait de leurs données ; d'assurer la maîtrise de leurs données, en facilitant l'exercice de leurs droits". Pour les personnes qui sont responsables du traitement, cela contribue à un "traitement loyal des données et permet d'instaurer une relation de confiance avec les personnes concernées".

L'article 34 de la loi Informatique et Libertés énonce que "le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données, et notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès".

ENGAGEMENT

N°17

JE PROGRESSE

Que dois-je faire pour atteindre le niveau 1 ?

Le personnel est formé et sensibilisé à l'usage légal des données personnelles. La déclaration CNIL pour la vidéosurveillance est faite et est à jour.

L'entreprise a des devoirs et des engagements vis-à-vis des clients qui lui font confiance en lui fournissant leurs données personnelles (nom, prénom, adresse, courriel et parfois même leur téléphone et leur adresse postale). Ainsi, la collecte de ce type de données rentre dans le cadre défini par le RGPD.

Pour faciliter la mise en place du RGPD, il est conseillé par la CNIL de désigner un ambassadeur de protection des données, appelé délégué à la protection des données personnelles ou Data Protection Officers (DPO) qui pourra être en mesure d'informer sur la collecte, le traitement et la gestion des données personnelles.

De plus, la CNIL précise que " Un employeur ne peut pas installer des caméras dans ses locaux sans définir un objectif, qui doit être légal et légitime ". Ainsi l'accès aux images de vidéosurveillance n'est pas ouvert à tous, seuls les responsables de la sécurité et la direction du point de vente peuvent avoir accès aux vidéos. Il faut donc déposer une demande d'autorisation de vidéosurveillance à la préfecture du lieu d'implantation du PDV.

Que dois-je faire pour atteindre le niveau 2 ?

Le point audité est conforme à la loi RGPD de l'UE applicable à compter du 25 mai 2018.

Il est conseillé, selon la CNIL, de réaliser en amont une analyse des activités de l'entreprise pour identifier qui collecte, traite et gère les données personnelles (le service RH gestion de la paie, du recrutement, formation, ...).

Pour valider votre analyse et répondre à la réglementation (article 30 RGPD) vous devrez centraliser cette information dans un registre qui doit comporter 3 types d'information :

- L'objectif poursuivi de cette collecte de données.
- Les catégories de données utilisées.
- Les personnes qui auront accès aux données collectées ainsi que la durée de conservation de ces données.

Par la suite, pour répondre aux obligations d'information et de transparence imposées par le RGPD, (article 12, 13 & 14) vous devez informer que vous collectez des données personnelles, et fournir les éléments suivants :

- La finalité de cette collecte.
- Le responsable du traitement de la donnée (identité et coordonnées de l'organisme).
- La base légale du traitement de la donnée (consentement des personnes par exemple).
- Si la collecte est obligatoire ou facultative.
- Le/les destinataires des données.
- La durée de conservation des données.
- Les droits des personnes concernées (droits d'accès, de rectification, effacement et limitations, et le droit d'introduire une réclamation à la CNIL).
- Les coordonnées de la personne chargée de la protection des données personnelles.

Pour répondre à cette dernière obligation vous pouvez mettre en place un formulaire de contact avec un numéro de téléphone et une adresse courriel qui permet le traitement rapide des demandes (droits d'accès, de rectification, d'opposition, d'effacement, à la portabilité et à la limitation du traitement) qui peuvent vous être adressées.

Attention : Il faut signaler à la CNIL les violations de données personnelles et ce, dans les 72h heures si cette violation est susceptible de représenter une menace pour les droits et libertés des personnes concernées.

Que dois-je faire pour atteindre le niveau 3 ?

Une zone de confidentialité est prévue dans les lieux d'échange de données personnelles.

L'accès aux données personnelles doit être défini par le biais d'une procédure qui doit être transmise à toutes les personnes qui sont en charge de la collecte, du traitement et de la gestion des données personnelles. L'accès aux données personnelles doit être restreint aux personnes qui sont formées et chargées du traitement et de la gestion des données.

L'aménagement d'une zone de confidentialité physique en magasin lors de la collecte des données personnelles est nécessaire. Cette zone "sécurisée" permet de ne pas diffuser ou divulguer les données personnelles récoltées. Cette zone doit permettre une récupération des données personnelles en toute sécurité pour que personne de non-autorisé n'ai accès aux données, ne les entende ou ne les voit.

ENGAGEMENT

N°17

JE PROGRESSE

Que dois-je faire pour atteindre le niveau 4 ?

Mise en place d'un suivi régulier.

La mise en place d'un suivi régulier du nombre de données collectées est nécessaire. Le registre va servir de tableau de suivi et donc de pilotage pour la gestion des données personnelles de vos parties prenantes.

De même, la mise en place d'un suivi régulier du nombre de personnes formées et du taux de conformité du magasin au RGPD est également nécessaire ; et là encore le registre va servir de tableau de suivi.

En effet, mettre à jour régulièrement votre registre vous permet d'anticiper les comportements non conformes à vos procédures et ainsi vous pouvez ajuster en renforçant par exemple les formations sur la gestion des données personnelles.

Les Éco-gestes :

Voici quelques bonnes pratiques proposées par la CNIL :

- Les comptes utilisateurs internes et externes sont-ils protégés par des mots de passe d'une complexité suffisante ?
- Les accès aux locaux sont-ils sécurisés ?
- Des profils distincts sont-ils créés selon les besoins des utilisateurs pour accéder aux données ?
- Avez-vous mis en place une procédure de sauvegarde et de récupération des données en cas d'incident ?''

Les ressources

https://www.francenum.gouv.fr/comprendre-le-numerique/autodiagnostic-rgpd-votre-tpe-pme-est-elle-en-conformite
https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-guide-rgpd-tpe-pme.pdf
https://www.cnil.fr/fr/rgpd-par-ou-commencer
https://www.cnil.fr/fr/conformite-rgpd-information-des-personnes-et-transparence
https://www.cnil.fr/sites/default/files/atoms/files/registre_rgpd_basique.pdf
https://www.cnil.fr/sites/default/files/atoms/files/guide_durees_de_conservation.pdf
https://www.cnil.fr/sites/default/files/atoms/files/affiche-plus_de_droits.pdf
https://www.cnil.fr/fr/la-cnil-publie-un-nouveau-modele-de-registre-simplifie
https://www.ca-moncommerce.com/creation-site-internet/rgpd-commercant-comment-sy-conformer/https://www.zdnet.fr/actualites/comment-la-mie-caline-a-externalise-la-fonction-dpo-39898395.htm
https://www.cnil.fr/fr/services-en-ligne
https://www.cnil.fr/fr/les-durees-de-conservation-des-donnees

ENGAGEMENT

N°17

LES EXEMPLES

LA MIE CÂLINE

La Mie Câline a fait le choix d'externaliser la fonction de DPO (Data Protection Officers), c'est-à-dire la personne chargée des données personnelles traitées.

Auparavant La Mie Câline gérait les démarches de déclaration à la CNIL en interne mais avec la RGPD tout a changé et cette démarche est devenue trop lourde.

De même, elle est constituée de nombreux établissements franchisés et il était trop compliqué de mettre en place la structure pour créer le poste de DPO en interne. Suite à cela, La Mie Câline a décidé de passer par un prestataire externe, Digimetis pour prendre en charge ce poste.

Cependant La Mie Câline reste le référent technique et Digimetis reste dans l'accompagnement et le conseil, ils font " en quelque sorte de l'audit des différents services ".

ENGAGEMENT N°17

LES ÉLÉMENTS DE PREUVES

Ma check-list pour préparer l'audit :

✔ NIVEAU 1 :

• Les supports de communication pour sensibiliser les collaborateurs.
• La déclaration à la préfecture de la vidéosurveillance.
• Le nom de la personne en charge de la protection des données.

✔ NIVEAU 2 :

• Le registre RGPD (le rapport de l'analyse des activités de l'entreprise).
• Formulaire de contact (numéro de téléphone, adresse courriel).

✔ NIVEAU 3 :

• Photo de la zone de confidentialité est prévue dans les lieux d'échanges de données personnelles.

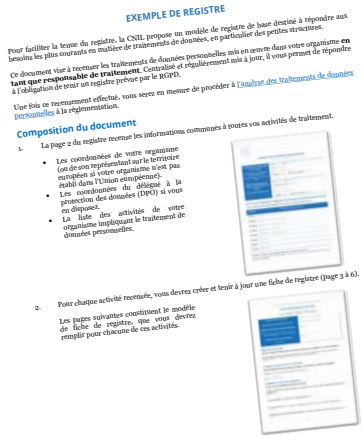
✔ NIVEAU 4 :

• Le tableau de suivi du nombre de données collectées (le registre RGPD sert de tableau de suivi).
• Suivi du nombre de personnes formées
• Le taux de conformité du magasin au RGPD.

1

2

3


EXEMPLE DE REGISTRE

Pour faciliter la tenue du registre, la CNIL propose un modèle de registre de base destiné à répondre aux besoins les plus courants en matière de traitements de données, en particulier des petites structures.

Ce document vise à recenser les traitements de données personnelles mis en œuvre dans votre organisme **en tant que responsable de traitement**. Centralisé et régulièrement mis à jour, il vous permet de répondre à l'obligation de tenir un registre prévue par le RGPD.

Une fois ce recensement effectué, vous serez en mesure de procéder à l'analyse des traitements de données personnelles à la réglementation.

Composition du document

1. La page 2 du registre recense les informations communes à toutes vos activités de traitement.
   - Les coordonnées de votre organisme (et de son représentant sur le territoire européen si votre organisme n'est pas établi dans l'Union européenne).
   - Les coordonnées du délégué à la protection des données (DPO) si vous en disposez.
   - La liste des activités de votre organisme impliquant le traitement de données personnelles.

2. Pour chaque activité recensée, vous devrez créer et tenir à jour une fiche de registre (page 3 à 6).

   Les pages suivantes constituent le modèle de fiche de registre, que vous devrez remplir pour chacune de ces activités.

4

5

Les exemples à fournir :

1. Affiche plus de droits
2. Droit accès-infographie
3. Registre RGPD basique
4. Exemple registre RGPD
5. Panneau zone de confidentialité suspendu