RGPD

Quelles obligations pour les entreprises alimentaires de proximité?

Le 25 mai 2018 est entré en application le règlement européen général sur la protection des données (RGPD).

Ce règlement vise à mieux protéger les données personnelles détenues notamment par les entreprises dans le cadre du développement du numérique (commerce en ligne, abonnement à une newsletter, …).

Les entreprises doivent s'assurer que toutes les données personnelles qu'elles collectent dans le cadre de leur activité (coordonnées de la clientèle, données du personnel, …) sont protégées, peuvent faire l'objet de modifications à la demande de la personne concernée, …

Les conséquences du RGPD en bref :

- Une opportunité pour renforcer la confiance

Toute personne qui confie à une entreprise ses données personnelles établit avec elle une relation de confiance. Elle souhaite le respect de ses droits et de sa vie privée.

Le RGPD confère en conséquence les droits suivants aux personnes pour maîtriser leurs données :

- droits d'accès,
- droits de rectification,
- droits d'effacement,
- droits d'opposition, etc.

- Une réflexion à engager sur les données à collecter

La mise en œuvre du RGPD conduit l'entreprise à se demander si chaque donnée collectée est bien nécessaire. En effet, l'entreprise ne doit collecter que les données nécessaires à la réalisation de son activité.

- La sécurisation des données

Que ces données soient stockées informatiquement ou sur papier, elles doivent faire l'objet de mesures de sécurité particulières.

Quelques définitions

- Donnée personnelle : «Toute information se rapportant à une personne physique identifiée ou identifiable».
    - Ex. : nom, prénom, numéro de téléphone, numéro de sécurité sociale, photo, …

- Traitement de données : «opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement) ».

  La gestion « papier » de traitement de données est concernée également.

    - Ex. : la gestion de données pour la livraison d'un client ou pour établir une carte de fidélité constitue un traitement de données.

  Un traitement de données doit avoir un objectif, une finalité. Une entreprise ne peut pas collecter ou traiter des données personnelles simplement au cas où cela lui serait utile un jour. À chaque traitement de données doit être assigné un but, qui doit bien évidemment être légal et légitime au regard de l'activité professionnelle.
    - Ex. : ne pas demander à un client de renseigner ses coordonnées postales dans le cadre de l'inscription à une newsletter destinée à l'informer des actualités de l'entreprise

Comment conduire sa mise en conformité RGPD ?

- Recenser, en créant un registre, les fichiers traitant des données personnelles et établir pour chaque fichier :
    - finalité du fichier (ex. : fichier « clients »),
    - données collectées, personnes ayant accès aux données (comptable, chef d'entreprise, …),
    - durée de conservation des données.
  - Ex. : plus d'informations sur le registre https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement
- Vérifier pour chaque fichier la pertinence des données collectées, les mettre à jour si nécessaire, supprimer les données dont le délai de conservation est dépassé, vérifier la sécurisation d'accès aux données.
- Respecter les droits des personnes : lors de la collecte de données, les personnes doivent savoir ce que l'entreprise va en faire, combien de temps elle va les garder, qui y aura accès, … Elles doivent être informées de comment elles peuvent exercer leurs droits sur les données.
  - Ex. de mentions à préciser : https://www.cnil.fr/fr/conformite-rgpd-information-des-personnes-et-transparence
  - Plus d'informations sur les droits des personnes : https://www.cnil.fr/fr/respecter-les-droits-des-personnes
- Sécuriser les données : limiter l'accès aux données au personnel en ayant besoin ; vérifier la sécurisation de l'outil informatique (mot de passe complexe et changé régulièrement, logiciel antivirus à jour, …).
  - Plus d'informations : https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf
  - En cas de violation de données personnelles susceptible de présenter un risque pour les droits et libertés des personnes concernées, il faut faire une déclaration en ligne à la CNIL[1] sous 72 h : https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

Dans le cas des entreprises alimentaires de proximité, ce registre concerne uniquement : les traitements non occasionnels (exemple : gestion de la paie, gestion des clients/prospects et des fournisseurs, etc.) ; les traitements susceptibles de comporter un risque pour les droits et libertés des personnes (exemple : systèmes de géolocalisation, de vidéosurveillance, etc.) ; les traitements qui portent sur des données sensibles (appartenance syndicale, origine ethnique, …)

En résumé :

- Ne collecter que les données vraiment nécessaires.
- Etre transparent.
- Penser aux droits des personnes.
- Garder la maîtrise des données.
- Identifier les risques.
- Sécuriser les données.

[1] Commission Nationale de l'Informatique et des Libertés

Les données du personnel

De nombreuses données personnelles relatives aux salariés des entreprises sont collectées pour notamment :

- la rémunération et les déclarations sociales
- la gestion administrative du personnel (coordonnées des personnes à prévenir en cas d'urgence, permis de conduire pour les livreurs, …)
- l'organisation du travail (photographie des salariés pour illustrer le site internet de l'entreprise, …)
- l'action sociale prise en charge par l'entreprise (informations sur les ayant-droit des salariés pour la mutuelle, …)

Bonnes pratiques :

- Ne demander que les informations utiles au fonctionnement de l'entreprise.
- Ne pas traiter de données sensibles liées aux salariés (appartenance syndicale, origine ethnique, …) qui demandent un traitement particulier.
- Assurer la confidentialité et la sécurité des données fournies.
- Informer les salariés de leurs droits à chaque demande de données.
- Sensibiliser les salariés à la confidentialité et à la sécurité des données détenues par l'entreprise.
- Ne pas oublier que les salariés peuvent demander une copie de toutes les données les concernant détenues par l'entreprise.

Plus d'informations sur : https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-rgpd_fiche_3_protegez-les-donnees-de-vos-collaborateurs.pdf

Remarques :

- La CNIL a rédigé des fiches spécifiques sur la géolocalisation des véhicules de l'entreprise, sur la videosurveillance en entreprise, … Plus d'informations sur https://www.cnil.fr/sites/default/files/atoms/files/travail-vie_privee.pdf
- La gestion des données évoquées ci-dessus concerne également les données collectées dans le cadre d'un recrutement.

Communication et/ou vente sur internet

- **Dans le cas d'un site vitrine** *(présentation de l'entreprise, abonnement éventuel à une newsletter, formulaire de contact)*
    - Doivent apparaitre sur le site des mentions CNIL en bas du formulaire de contact, un moyen de contact permettant aux internautes d'exercer leurs droits par voie électronique, des mentions légales identifiant l'éditeur du site. Plus d'informations sur https://www.service-public.fr/professionnels-entreprises/vosdroits/F31228
    - Si le site internet dépose des cookies ou des traceurs, il faut informer l'internaute ou lui demander son consentement. Plus d'informations sur https://www.cnil.fr/fr/site-web-cookies-et-autres-traceurs

- **Dans le cas de vente en ligne**
    - Ne collecter que les données nécessaires sur le client.
        - Ex. : ne pas lui demander sa date de naissance si rien n'est prévu (remise, cadeau, …) lors de sa date d'anniversaire.
    - Faire apparaitre une mention lors de la vente sur l'information et le consentement du client par rapport à l'utilisation de ses données.
    - Sécuriser les données en ligne :
        - La vente doit se faire sous « https:// »
        - Ne pas conserver les données bancaires des clients.
        - Demander un mot de passe complexe pour le compte client.
        - Ne transmettre par mail au client aucune donnée de sécurité telle le mot de passe.
        - Sécuriser la transaction bancaire.
        - Plus d'information sur https://www.cnil.fr/fr/securite-securiser-les-sites-web

- **Communication sur les réseaux sociaux**
    - Prévoir un lien ou un article permettant à l'internaute d'avoir l'information sur les droits.
    - Prévoir une réponse type aux internautes mécontents à envoyer rapidement (e-réputation).

Bonnes pratiques :

- Ne collecter que les informations nécessaires.
- Informer l'internaute des modalités mises en œuvre pour exercer ses droits par rapport à ses données.
- Obtenir son consentement par rapport au traitement de ses données.
- Sécuriser les données (compte client, transaction bancaire, …)
- Plus d'informations sur https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-rgpd_fiche-1_que-faire-quand-votre-entreprise-communique-vend-en-ligne.pdf

Prospection et gestion des fichiers « clients »

- Prospection de nouveaux clients :
  - Pour faire du démarchage commercial, ne pas utiliser les coordonnées personnelles en libre accès dans des annuaires par exemple. En effet, les personnes peuvent être inscrites sur des listes anti-démarchage comme bloctel (http://www.bloctel.gouv.fr/).
  - N'avoir recours qu'à des bases de données marketing fiables.
  - Ne pas utiliser celles à prix attractif vendues sur internet. Ceci évitera toute plainte auprès de la CNIL par des personnes mécontentes d'avoir été démarchées.
  - Plus d'informations sur https://pro.bloctel.fr/
- Recueil du consentement des clients
  - Que ce soit pour les nouveaux ou les anciens clients, nécessité de permettre aux personnes de refuser de recevoir d'autres sollicitations de l'entreprise.
  - Plus d'informations sur https://www.cnil.fr/fr/les-regles-dor-de-la-prospection-par-courrier-electronique-0
- Collecte et gestion des données des clients :
  - Ne collecter que les informations nécessaires.
  - Ne pas garder en mémoire les données d'usage ponctuel.
  - Informer les clients de l'usage que l'entreprise fait des données collectées.
    - Ex. : prévoir sur le site internet de l'entreprise un chapitre sur la protection des données dans les conditions générales de vente par exemple.
    - Ex. : mention d'information à faire figurer sur chaque formulaire de collecte.
  - Prévoir la suppression des informations en cas « d'inactivité prolongée des clients » sauf celles en lien avec la conservation légale de documents (comptabilité, …).
  - Plus d'informations sur https://www.cnil.fr/sites/default/files/atoms/files/commerce_et_donnees_personelles.pdf

Bonnes pratiques :

- Ne pas démarcher des personnes répertoriées sur des listes d'opposition au démarchage.
- N'avoir recours qu'à des bases de données fiables.
- Ne collecter que les informations nécessaires.
- Informer le client des modalités lui permettant d'exercer ses droits par rapport à ses données.
- Obtenir son consentement par rapport au traitement de ses données.
- Plus d'informations sur https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-rgpd_fiche_2_ameliorez-maitrisez-votre-relation-client_0.pdf

Pour plus d'informations : https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-guide-rgpd-tpe-pme.pdf