Chambres de Métiers et de l'Artisanat
Région Centre-Val de Loire

ARTISANS, êtes-vous prêts ?

RGPD
MODE D'EMPLOI

PETIT **HISTORIQUE**

2018 : RGPD.

1995 : Directive 95/46/CE : sur la protection des données à caractère personnel.

1978 : Loi informatique et liberté : relative à l'informatique, aux fichiers et aux libertés.

1803 : Article 9 du code civil : droit au respect de sa vie privée

RGPD, **POURQUOI ?**

Uniformisation des règles

Renforcement des droits des personnes

Responsabilisation des acteurs

QUI EST CONCERNÉ **PAR LE RGPD ?**

Toute entité publique ou privée collectant des données à caractère personnel sur le territoire de l'UE et toute organisation hors UE proposant des biens et services à des personnes basées sur le territoire de l'UE.

Chambre régionale de Métiers et de l'Artisanat du Centre-Val de Loire
28 rue du Faubourg Bourgogne - 45000 ORLÉANS
02 38 68 03 32 - contact-crma@crma-centre.fr - www.crma-centre.fr

QU'EST-CE QU'UNE «DONNÉE À CARACTÈRE PERSONNEL ?»

Il s'agit de toute information permettant de reconnaître ou identifier une personne, directement ou indirectement.

C'est donc : nom, prénom, adresse postale et électronique, téléphone, numéro de sécurité sociale, de carte bancaire, revenus, plaque d'immatriculation, mots de passe, adresse IP, historique de navigation web, de tchat, de géolocalisation, photo...

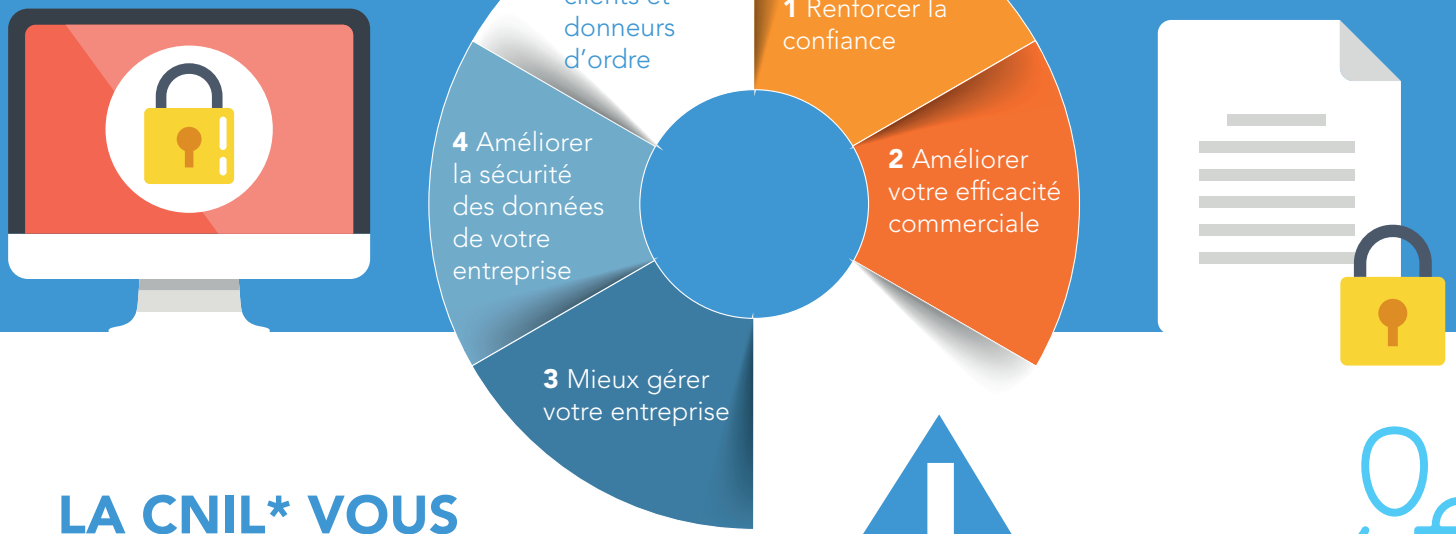
Leur divulgation ou leur mauvaise utilisation peut porter atteinte aux droits et libertés des personnes et à leur vie privée. Ces données à caractère personnel peuvent se retrouver partout en entreprise notamment dans les contrats, fiches de paie, formulaires, documents relatifs à la santé, casiers judiciaires, trombinoscopes, badges d'accès, matériels informatiques pro, répertoire mail interne de l'entreprise, documents commerciaux (devis, factures, fiches d'intervention…), documents bureautiques, bases de données clients...

QU'ENTEND-T-ON PAR «TRAITEMENT DE DONNÉES PERSONNELLES ?»

Il est fait référence à toute action effectuée sur des données à caractère personnel de personnes physiques.

- collecte d'informations via une fiche de renseignements, un bordereau d'inscription, un questionnaire, un formulaire de contact, un formulaire d'inscription à une newsletter…
- enregistrement d'une base de données, d'un fichier clients par exemple…
- mise à jour d'un fichier fournisseurs,
- mise en place d'un système de vidéosurveillance

QUELLES OPPORTUNITÉS OFFRENT LE RGPD AUX ENTREPRISES ?



LA CNIL* VOUS RECOMMANDE 4 ÉTAPES PRINCIPALES À MENER POUR ENTAMER VOTRE MISE EN CONFORMITÉ

*Commission Nationale de l'Informatique et des Libertés

Avant de débuter toute action, le choix d'un DPO (délégué à la protection des données) peut se faire pour les petites entreprises. Un DPO peut être choisi à l'extérieur de l'entreprise et à plusieurs ! Il est obligatoire pour les organismes publics ; les organisations faisant de la surveillance de personne à grande échelle et les organisations gérant des données sensibles.

1 CONSTITUEZ UN REGISTRE DE TRAITEMENT DE VOS DONNÉES

Pour les entreprises de moins de 250 salariés ne doivent inscrire sur ce registre que les traitements suivants :

- les traitements non occasionnels : gestion de la paie, fichiers clients, fichiers fournisseurs…
- les traitements susceptibles de comporter un risque pour les droits et libertés des personnes : vidéosurveillance, systèmes de géolocalisation…
- les traitements qui portent sur des données sensibles.

Par ailleurs, si vous opérez des traitements en tant que sous-traitant pour le compte de clients, vous devez mettre en place un second registre : le registre du sous-traitant.

Téléchargez notre exemple de registre de données

Téléchargez le guide du sous-traitant de la CNIL

Ce qui change vraiment avec le RGPD

Informations à donner avant le RGPD :

- **Identité** et coordonnées de l'**organisme** (responsable du traitement de données) ;
- **Finalités** (à quoi vont servir les données collectées) ;
- Caractère obligatoire ou facultatif du **recueil des données** (ce qui suppose une réflexion en amont sur l'utilité de collecter ces données au vu de l'objectif poursuivi – principe de « minimisation » des données) et conséquences pour la personne en cas de non-fourniture des données ;
- **Destinataires ou catégories de destinataires** des données (qui a besoin d'y accéder ou de les recevoir au vu des finalités définies) ;
- Durée de **conservation des données** (ou critères permettant de la déterminer) ;
- **Droits des personnes concernées** (opposition, accès, rectification, effacement ; nouveaux droits RGPD : limitation, portabilité) ;

Informations supplémentaires à donner après le RGPD :

- Coordonnées du **délégué à la protection des données** de l'organisme, s'il a été désigné, ou d'un point de contact sur les questions de protection des données personnelles ;
- **Base juridique du traitement** de données (c'est-à-dire ce qui autorise légalement le traitement : il peut s'agir du consentement des personnes concernées, du respect d'une obligation prévue par un texte, de l'exécution d'un contrat, etc.) ;
- Droit d'introduire une **réclamation** (plainte) auprès de la CNIL ;

2 FAITES LE TRI DANS VOS DONNÉES

En minimisant la collecte de données, en éliminant de vos formulaires de collecte et vos bases de données toutes les informations inutiles. Redéfinissez qui doit pouvoir accéder à quelles données dans votre entreprise. Pensez à poser des règles automatiques d'effacement ou d'archivage au bout d'une certaine durée dans vos applications.

Mémo à retrouver dans le registre de traitement des données

3 RESPECTEZ LES DROITS DES PERSONNES QUE VOUS SOLLICITEZ EN INTERNE ET EN EXTERNE DE L'ENTREPRISE

Elles doivent en effet savoir ce que vous allez faire de leurs données, donner leur consentement au traitement et être en mesure d'exercer facilement leurs droits.

A chaque fois que vous collectez des données personnelles, le support utilisé (formulaire, questionnaire, etc.) doit ainsi comporter certaines informations :

- identité et coordonnées du responsable du traitement (ou de son représentant),
- finalités du traitement effectué,
- base juridique du traitement,
- destinataires des données,
- durée de conservation des données,
- droit d'introduire une réclamation auprès d'une autorité de contrôle,
- etc.

Vous devez respecter les 4 principes fondamentaux du RGPD :

- le consentement qui doit être recueilli et prouvé,
- le droit à l'information indispensable à l'expression du consentement,
- le droit à l'oubli ou à l'effacement des données personnelles,
- le droit à la portabilité c'est-à-dire le fait de récupérer ses données pour les transférer à un tiers.

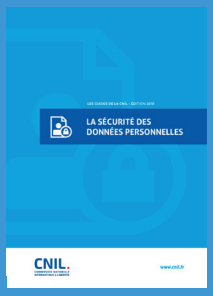
Téléchargez notre exemple

4 SÉCURISEZ VOS DONNÉES

Pensez à mettre régulièrement à jour vos logiciels et antivirus, changez régulièrement de mots de passe, etc.

Vous êtes en effet tenu à une obligation légale d'assurer la sécurité des données personnelles que vous détenez. Pour évaluer le niveau de sécurité des données personnelles dans votre entreprise, voici quelques questions à se poser :

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 ?



Téléchargez le guide de sécurité des données créé par la CNIL

RISQUES ET SANCTIONS EN CAS DE NON-RESPECT DU RGPD

Seront responsables du traitement des données les entreprises et institutions, mais aussi les prestataires informatiques et donneurs d'ordre. Ainsi, il ne sera pas possible de déléguer ses responsabilités à d'autres entités.

D'abord, des sanctions administratives et pénales pourront être mises en place en fonction de la gravité du manquement. Mais aussi des sanctions financières à hauteur de 2% à 4% du CA ou de 10 000 000 à 20 000 000€ en fonction du manquement également. En France, c'est la Commission nationale de l'informatique et des libertés (Cnil) qui veillera à la bonne application du RGPD.

Pour en savoir plus : www.cnil.fr

Si vous souhaitez aller plus loin et faire une analyse des impacts : ici

Sachez quoi faire quand votre entreprise communique et/ou vend en ligne : ici

Améliorez et maîtrisez votre relation client : ici

Protégez les données de vos collaborateurs : ici

L'EUROPE s'engage en région Centre-Val de Loire avec le FEDER

L'Europe s'engage en région Centre-Val de Loire avec le soutien du FEDER

Centre-Val de Loire
www.regioncentre-valdeloire.fr