PROTECTION DES DONNÉES PERSONNELLES

Comment passer à l'action ?

Selon la CNIL, quatre actions principales sont à mener pour entamer votre mise en conformité aux règles de protection des données. Voyons lesquelles.

1. Recensez vos fichiers

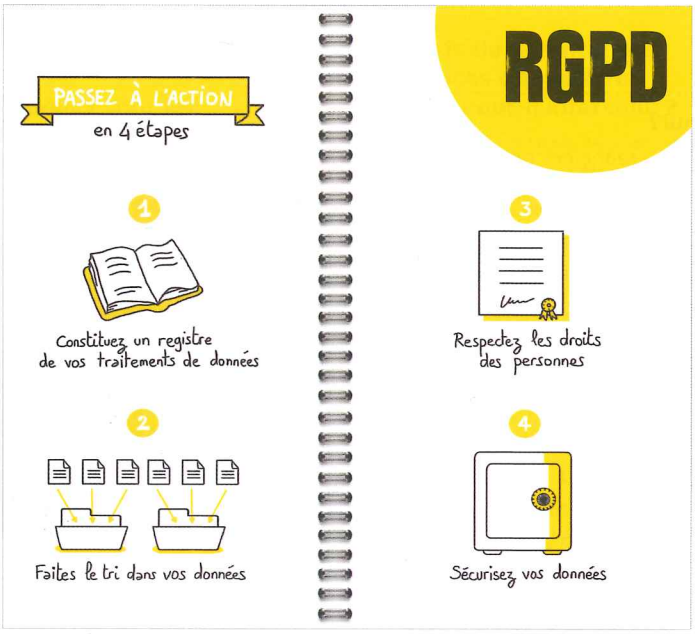
Identifiez les activités principales de votre entreprise qui nécessitent la collecte et le traitement de données (recrutement, gestion de la paie, formation, gestion des badges et des accès, statistiques de vente, gestion des clients et prospects...).

Dans un registre de traitement des données[1], créez une fiche pour chaque activité recensée, en précisant :
- l'objectif poursuivi (la finalité – exemple : la fidélisation client) ;
- les catégories de données utilisées (exemples pour la paie : nom, prénom, date de naissance, salaire...) ;
- qui a accès aux données (le destinataire – exemples : service chargé du recrutement, service informatique, direction, prestataires, partenaires, hébergeurs) ;
- la durée de conservation de ces données.

2. Faites le tri dans vos données

Pour chaque fiche de registre créée, vérifiez que :
- les données que vous traitez sont nécessaires à vos activités ;
- vous ne traitez aucune donnée dite « sensible » ou, si c'est le cas, que vous avez bien le droit de les traiter ;
- seules les personnes habilitées ont accès aux données dont elles ont besoin ;
- vous ne conservez pas vos données au-delà de ce qui est nécessaire.

La CNIL conseille d'améliorer ses pratiques en minimisant la collecte de données et en éliminant de vos formulaires de collecte et de vos bases de données toutes les informations inutiles.
Redéfinissez qui doit pouvoir accéder à quelles données dans l'entreprise.



Source : *Guide pratique de sensibilisation au RGPD pour les petites et moyennes entreprises*, CNIL, Bpifrance.

Pensez à poser des règles automatiques d'effacement ou d'archivage au bout d'une certaine durée dans vos applications...

3. Respectez les droits des personnes

Informez les personnes
À chaque fois que vous collectez des données personnelles, le support utilisé (formulaire, questionnaire, etc.) doit comporter des mentions d'information :
- **pourquoi vous collectez les données** (« la finalité » ; par exemple, gérer l'achat en ligne du consommateur) ;
- **ce qui vous autorise à traiter ces données** (le « fondement juridique » : il peut s'agir du consentement de la personne concernée, de l'exécution d'un contrat, du respect d'une obligation légale qui s'impose à vous, de votre « intérêt légitime ») ;
- **qui a accès aux données** (indiquez des catégories : les services internes compétents, un prestataire, etc.) ;
- **combien de temps vous les conservez** (exemple : cinq ans après la fin de la relation contractuelle) ;
- **les modalités selon lesquelles les personnes concernées peuvent exercer leurs droits** (dans leur espace personnel sur votre site Internet, par un message à une adresse e-mail spécifique, par un courrier postal à un service identifié...) ;
- **si vous transférez des données hors de l'Union européenne** (précisez le pays et l'encadrement juridique qui maintient le niveau de protection des données).

Des exemples de mentions sont disponibles sur le site Internet de la CNIL et dans les fiches pratiques de la FFB[2].
Pour éviter des mentions trop longues dans un formulaire en ligne, vous pouvez, par exemple, donner un premier niveau d'information en fin de formulaire et renvoyer à une politique de confidentialité ou à une page vie privée sur votre site Internet.

Permettez aux personnes d'exercer facilement leurs droits
Les personnes dont vous traitez les données (clients, collaborateurs, prestataires, etc.) ont des droits sur leurs données : droit d'accès, de rectification, d'opposition, d'effacement, droit à la portabilité et à la limitation du traitement.

Vous devez leur donner les moyens d'exercer effectivement leurs droits. Si vous disposez d'un site Web, prévoyez un formulaire de contact, un numéro de téléphone ou une adresse de messagerie spécifiques. Si vous proposez un compte en ligne, donnez à vos clients la possibilité d'exercer leurs droits à partir de leur compte.

Mettez en place un processus interne garantissant l'identification et le traitement des demandes dans des délais courts (un mois au maximum).

4. Sécurisez vos données

Garantissez l'intégrité de votre patrimoine de données en minimisant les risques de perte de données ou de piratage.

Les mesures à prendre sont informatiques et physiques : mise à jour de vos antivirus et logiciels, utilisation de mots de passe complexes et changement régulier, chiffrement de vos données dans certaines situations, verrouillage des locaux abritant les données personnelles, etc.

1. Cf. *Bâtiment actualité* n° 4 du 7 mars 2018. Un modèle de registre est disponible, en version Excel, sur le site de la CNIL.
2. Disponibles auprès de votre fédération.