Le RGPD en pratique

4 actions principales :

- La tenue d'un registre

En pratique, une fiche de registre doit être établie.

Ce registre doit comporter **le nom et les coordonnées de votre organisme** ainsi que, le cas échéant, de votre représentant, si votre organisme n'est pas établi dans l'Union européenne.

En outre, **pour chaque activité de traitement,** la fiche de registre doit comporter au moins les éléments suivants :

1. L'objectif poursuivi : la finalité de la collecte, par exemple la fidélisation client
2. les catégories **de personnes concernées** (client, prospect, employé, etc.)
3. les catégories de **données personnelles** (exemples : identité, situation familiale, économique ou financière, données bancaires, données de connexion, donnés de localisation, etc.)
4. **les catégories de destinataires** auxquels les données à caractère personnel ont été ou seront communiquées, y compris les sous-traitants auxquels vous recourez
5. La durée de conservation de ces données

Vous trouverez un modèle de registre à l'adresse suivante :
https://www.cnil.fr/sites/default/files/atoms/files/registre_rgpd_basique.pdf

- Faites le tri dans vos données

Pour chaque fiche de registre créée, vérifiez :

• que les données que vous traitez sont nécessaires à vos activités (par exemple, il n'est pas utile de savoir si vos salariés ont des enfants, si vous n'offrez aucun service ou rémunération attachée à cette caractéristique) ;
• que vous ne traitez aucune donnée dite « sensible » ou, si c'est le cas, que vous avez bien le droit de les traiter;
• que seules les personnes habilitées ont accès aux données dont elles ont besoin ;
• que vous ne conservez pas vos données au-delà de ce qui est nécessaire.

L'idée ici est de minimiser la collecte de données, en éliminant de vos formulaires de collecte et vos bases de données toutes les informations inutiles.

- Respecter le droit des personnes

À chaque fois que vous collectez des données personnelles, le support utilisé (formulaire, questionnaire, etc.) doit comporter des mentions d'information.

Vérifiez que l'information comporte notamment les éléments suivants :

• pourquoi vous collectez les données (« la finalité » ; par exemple pour 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 : « 5 ans après la fin de la relation contractuelle ») ;
• les modalités selon lesquelles les personnes concernées peuvent exercer leurs droits (via leur espace personnel sur votre site internet, par un message sur une adresse email dédiée, 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.

Pour éviter des mentions trop longues au niveau d'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/ page vie privée sur votre site internet.

À l'issue de cette étape, vous avez répondu à votre obligation de transparence.

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, qui sont d'ailleurs renforcés par le RGPD : droit d'accès, de rectification, d'opposition, d'effacement, 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 spécifique, un numéro de téléphone ou une adresse de messagerie dédiée. 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 permettant de garantir l'identification et le traitement des demandes dans des délais courts (1 mois au maximum).

- Sécuriser vos données :

Garantissez l'intégrité de votre patrimoine de données en minimisant les risques de pertes de données ou de piratage. Les mesures à prendre, informatiques ou physiques, dépendent de la sensibilité des données que vous traitez et des risques qui pèsent sur les personnes en cas d'incident.

Différentes actions doivent être mises en place : mises à jour de vos antivirus et logiciels, changement régulier des mots de passe et utilisation de mots de passe complexes, ou chiffrement de vos données dans certaines situations. En cas de perte ou vol d'un outil informatique, il sera plus difficile pour un tiers d'y accéder.

Signalez à la CNIL les violations de données personnelles :

Votre entreprise a subi une violation de données (des données personnelles ont été, de manière accidentelle ou illicite, détruites, perdues, altérées, divulguées ou vous avez constaté un accès non autorisé à des données) ? **Vous devez la signaler à la CNIL dans les 72 heures si cette violation est susceptible de représenter un risque pour les droits et libertés des personnes concernées.** Cette notification s'effectue en ligne sur le site internet de la CNIL. Si ces risques sont élevés pour ces personnes, vous devrez les en informer. À l'issue de cette étape, vous serez en capacité d'assurer une protection des données personnelles en continu et de faire face aux incidents.