RGPD : par où commencer

Les 4 actions principales à mener pour entamer et maintenir sa mise en conformité avec les règles de protection des données.

1. Constituez un registre de vos traitements de données

En constituant votre registre, vous aurez une vision d'ensemble sur vos traitements de données.

Identifiez les activités principales de votre entreprise qui utilisent des données personnelles.
Exemples : recrutement, gestion de la paye, formation, gestion des badges et des accès, statistiques de ventes, gestion des clients prospects, etc.

> **Appuyez-vous sur le modèle de registre.**

Dans votre registre, créez une fiche pour chaque activité recensée, en précisant :

- L'objectif poursuivi (exemple : la fidélisation client) ;
- **Les catégories de données utilisées** (exemple pour la paie : nom, prénom, date de naissance, salaire) ;
- **Qui a accès aux données** (exemple : service chargé du recrutement, service informatique, direction, prestataires, partenaires, hébergeurs) ;
- La durée de conservation de ces données (durée durant laquelle les données sont utiles d'un point de vue opérationnel, et durée de conservation en archive).

Le registre est placé sous la responsabilité du dirigeant de l'entreprise.

Pour avoir un registre exhaustif et à jour, il faut en discuter et être en contact avec toutes les personnes de l'entreprise susceptibles de traiter des données personnelles.

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 (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) ;
- vous ne traitez aucune donnée dite « sensible » ou, si c'est le cas, que vous avez bien le droit de les traiter (voir la fiche « Traitements de données à risque : êtes-vous concerné ? ») ;
- 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.

À cette occasion, améliorez vos pratiques ! Minimisez la collecte de données, en éliminant toutes les informations inutiles. Redéfinissez qui doit pouvoir accéder à quelles données dans votre entreprise. Définissez, quand cela est possible, des règles automatiques d'effacement ou d'archivage au bout d'une certaine durée dans vos applications.

3. Respectez les droits des personnes

Le RGPD renforce l'obligation d'information et de transparence à l'égard des personnes dont vous traitez les données (clients, collaborateurs, etc.).

Informez les 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 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'UE (précisez le pays et l'encadrement juridique qui maintient le niveau de protection des données).

> **Appuyez-vous sur** les exemples de mentions.

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 : 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).

Bonne pratique : soyez réactifs !

Bien traiter les demandes des consommateurs quant à leurs données personnelles, c'est :

- renforcer la confiance qui sécurise la relation-client ;
- vous mettre à l'abri de critiques sur les réseaux sociaux, ou de plaintes auprès de la CNIL.

À l'issue de cette étape, vous serez en capacité de répondre aux demandes des personnes concernées.

Pour en savoir plus : « Respecter les droits des personnes ».

4. Sécurisez vos données

Si le risque zéro n'existe pas en informatique, vous devez prendre les mesures nécessaires pour sécuriser les données.

Cela vous permet aussi de protéger votre patrimoine de données en réduisant 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 de d'incident.

Des réflexes doivent être mis en place : mettre à jour de vos antivirus et logiciels, bien choisir ses mots de passe, chiffrer vos données dans certaines situations et faire des sauvegardes.

Les failles de sécurité ont également des conséquences pour ceux qui vous ont confié des données personnelles : Ayez à l'esprit les conséquences pour les personnes et pour votre entreprise.

Exemple : vous êtes restaurateur et vous livrez à domicile. Vos clients vous communiquent leur adresse précise et le code d'entrée de leur immeuble. Si ces informations sont piratées ou perdues, elles peuvent être utilisées pour s'introduire frauduleusement au domicile de votre client. Conséquence désastreuse pour vos clients, mais aussi pour vous !

BONNE PRATIQUE

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 ?

Pour en savoir plus :

- Guide des bonnes pratiques de l'informatique réalisé par l'ANSSI et la CPME sur le site internet www.cybermalveillance.gouv.fr
- Guide sécurité des données personnelles de la CNIL

Pour vous aider en cas de difficultés (un sinistre, une attaque informatique, etc.), le site gouvernemental www.cybermalveillance.gouv.fr vous propose de l'aide en ligne ainsi qu'une liste de prestataires approuvés.

BONNE PRATIQUE

L'approche assurantielle au-delà du RGPD :

Cette démarche d'anticipation sur le niveau global de sécurité peut être complétée par une approche assurantielle. Renseignez-vous auprès de ces professionnels sur le contenu possible des polices d'assurance (responsabilité civile, dommages couverts…) et surtout sur les services à l'assuré (notamment l'assistance en cas de sinistre, de gestion de crise…).

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 web 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.

Un accompagnement spécifique des têtes de réseaux

Publié le 14 avril 2021

La démarche d'accompagnement consiste à assister les têtes de réseaux, tant dans leur production de guides pratiques qu'en répondant à leurs demandes de conseil spécifiques aux différents secteurs d'activité.

Au-delà, la CNIL accompagne les TPE et PME grâce à des partenariats avec :

- l'ordre des experts comptables en septembre 2020 ;
- le médiateur des entreprises, en septembre 2020 également ;
- France Num, la politique publique de transformation numérique des TPE, dont la CNIL est partenaire au même titre que les réseaux territoriaux (CCI, chambre d'artisanat, régions, Dirrecte, etc.) qui sont intégrés au maillage de l'écosystème des TPE et PME.

Enfin, la CNIL certifie des organismes et des référentiels de certification comme celui relatif aux compétences du DPO.

Document reference

Les documents à télécharger

Check-list RGPD pour les TPE-PME
[PDF-347.02 Ko]
Guide de sensibilisation au RGPD pour les petites et moyennes entreprises
[PDF-2.78 Mo]
FICHE 1 : Votre entreprise communique et/ou vend en ligne
[PDF-201.64 Ko]
FICHE 2 : Améliorez et maîtrisez votre relation client
[PDF-225.46 Ko]
FICHE 3 : Protégez les données de vos collaborateurs
[PDF-192.97 Ko]
Haut de page